

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-149413

(43) 公開日 平成11年(1999) 6月2日

(51) Int.Cl.⁶

G 0 6 F 12/14
12/00

識別記号

3 1 0
5 3 7

F I

G 0 6 F 12/14
12/00

3 1 0 Z
5 3 7 Z

審査請求 未請求 請求項の数29 O L (全 35 頁)

(21) 出願番号 特願平9-314017
(22) 出願日 平成9年(1997)11月14日

(71) 出願人 000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番1号
(72) 発明者 蒲田 順
神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
(72) 発明者 黒田 康嗣
神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
(72) 発明者 小野 越夫
神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
(74) 代理人 弁理士 大曾 義之 (外1名)

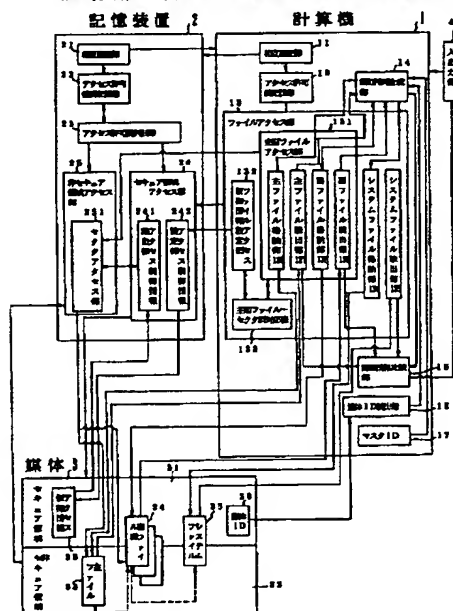
(54) 【発明の名称】 改ざん防止／検出機能を有するファイル管理システム

(57) 【要約】

【課題】 電子化されたデータファイルの改ざんを防止することが課題である。

【解決手段】 通常アクセスが許されないセキュア領域に、データファイルから生成した認証子を保存しておくことで、上記データファイルの改ざんを検出することができる。しかも、上記データファイルを主ファイルとし、主ファイルと関連付けられたさまざまな副ファイルから、上記認証子を生成することで、上記認証子を保存しておく上記セキュア領域のサイズは、小さくて済む。

本発明の実施の形態における改ざん防止／検出機能を有するファイル管理システムの全体構成図



【特許請求の範囲】

【請求項1】 計算機と記憶装置とを備えたファイルシステムであって、該計算機は、該記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、該アクセス許可鍵を格納するアクセス許可鍵記憶手段と、該アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手段と、を備え、該記憶装置は、該計算機との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、該アクセス許可鍵を格納するアクセス許可鍵群記憶手段と、該ファイルアクセス手段から送付され該アクセス許可鍵記憶手段に格納されたアクセス許可鍵と該アクセス許可鍵群記憶手段に格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手段と、該アクセス許可鍵判別手段が同一と判断した場合、通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手段と、を備えたファイル管理システム。

【請求項2】 請求項1に記載のファイル管理システムであって、前記計算機に備えられた相互認証手段および前記ファイルアクセス手段は、ハードウェアで実現されることを特徴とするファイル管理システム。

【請求項3】 主ファイルに関連付けられた一つまたは複数の副ファイルを格納する副ファイル格納手段と、該副ファイルの検証に使用する副ファイル認証情報を生成する認証情報生成手段と、該副ファイル認証情報を関連付けたシステムファイルを格納するシステムファイル格納手段と、を備えることを特徴とするファイル管理システム。

【請求項4】 主ファイルを格納する主ファイル格納手段と、該主ファイルの検証に使用する主ファイル認証情報を生成する認証情報生成手段と、該主ファイル認証情報を関連付けた少なくとも1つの副ファイルを格納する副ファイル格納手段と、を備えることを特徴とするファイル管理システム。

【請求項5】 主ファイルを格納する主ファイル格納手段と、該主ファイル認証情報を関連付けた少なくとも1つの副ファイルを格納する副ファイル格納手段と、該主ファイルの検証に使用する主ファイル認証情報および該副ファイルの検証に使用する副ファイル認証情報を生成する認証情報生成手段と、該副ファイル認証情報を関連付けたシステムファイルを

格納するシステムファイル格納手段と、を備えることを特徴とするファイル管理システム。

【請求項6】 請求項5において、前記主ファイル、前記副ファイルおよび前記システムファイルを通常アクセスできる非セキュア領域に格納することを特徴とするファイル管理システム。

【請求項7】 請求項5において、前記主ファイルを通常アクセスできる非セキュア領域に格納し、前記副ファイルおよび前記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システム。

【請求項8】 請求項5において、前記主ファイルおよび前記副ファイルを通常アクセスできる非セキュア領域に格納し、前記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システム。

【請求項9】 請求項6～8のいずれか1項記載のファイル管理システムであって、計算機と、

記憶装置とを更に備え、

該計算機は、該記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、該アクセス許可鍵を格納するアクセス許可鍵記憶手段と、該アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手段と、を備え、

該記憶装置は、該計算機との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、

該アクセス許可鍵を格納するアクセス許可鍵群記憶手段と、該アクセス許可鍵記憶手段に格納されたアクセス許可鍵と該アクセス許可鍵群記憶手段に格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手段と、

通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手段と、

を備え、

該認証情報生成手段は、

該相互認証の後、該セキュア領域に格納されている媒体固有の媒体IDを読み出し、該主ファイル認証情報および該副ファイル認証情報の生成に使用することを特徴とするファイル管理システム。

【請求項10】 請求項9に記載のファイル管理システムであって、前記計算機に備えられた相互認証手段および前記ファイルアクセス手段は、ハードウェアで実現されることを特徴とするファイル管理システム。

【請求項11】 請求項9または10に記載のファイル管理システムであって、

該媒体IDは、カードIDであることを特徴とするファイル管理システム。

【請求項12】 請求項9または10に記載のファイル管理システムであって、

該媒体IDは、マスタIDであることを特徴とするファイル管理システム。

【請求項13】 請求項9～12のいずれか1項記載のファイル管理システムであって、

前記認証情報の生成は、ファイルのレコードごとに行うことを特徴とするファイル管理システム。

【請求項14】 主ファイルに関連付けられた1つまたは複数の副ファイルを読み出す副ファイル読出手段と、該副ファイル読出手段から読み出された副ファイルから副ファイル認証情報を生成する認証情報生成手段と、該副ファイルに関連付けられたシステムファイルから副ファイル認証情報を読み出すシステムファイル読出手段と、

該認証情報生成手段が生成した副ファイル認証情報と該システムファイル読出手段が読み出した副ファイル認証情報とを比較する認証情報比較手段と、備えることを特徴とするファイル管理システム。

【請求項15】 主ファイルを読み出す主ファイル読出手段と、該主ファイル読出手段から読み出された主ファイルから主ファイル認証情報を生成する認証情報生成手段と、

該主ファイルに関連付けられた副ファイルから主ファイル認証情報を読み出す副ファイル読出手段と、

該認証情報生成手段が生成した主ファイル認証情報と該副ファイル読出手段が読み出した主ファイル認証情報とを比較する認証情報比較手段と、

備えることを特徴とするファイル管理システム。

【請求項16】 主ファイルを読み出す主ファイル読出手段と、

該主ファイルに関連付けられた副ファイルのうち主ファイル認証情報および該主ファイルに関連付けられた1つまたは複数の副ファイルを読み出す副ファイル読出手段と、

該副ファイルに関連付けられたシステムファイルから副ファイル認証情報を読み出すシステムファイル読出手段と、

該主ファイル読出手段から読み出された主ファイルから主ファイル認証情報を生成し、該副ファイル読出手段から読み出された副ファイルから副ファイル認証情報を生成する認証情報生成手段と、

該認証情報生成手段が生成した主ファイル認証情報と該副ファイル読出手段が読み出した主ファイル認証情報とを比較し、該認証情報生成手段が生成した副ファイル認証情報と該システムファイル読出手段が読み出した副ファイル認証情報とを比較する認証情報比較手段と、

を備えることを特徴とするファイル管理システム。

【請求項17】 請求項16において、前記主ファイル、前記副ファイルおよび前記システムファイルを通常アクセスできる非セキュア領域に格納することを特徴とするファイル管理システム。

【請求項18】 請求項16において、前記主ファイルを通常アクセスできる非セキュア領域に格納し、前記副ファイルおよび前記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システム。

10 【請求項19】 請求項16において、前記主ファイルおよび前記副ファイルを通常アクセスできる非セキュア領域に格納し、前記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システム。

【請求項20】 請求項17～19のいずれか1項記載のファイル管理システムであって、

計算機と、

記憶装置とを更に備え、

該計算機は、

20 該記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、

該アクセス許可鍵を格納するアクセス許可鍵記憶手段

と、該アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手段と、

を備え、

該記憶装置は、

該計算機との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、

該アクセス許可鍵を格納するアクセス許可鍵群記憶手段と、

30 該アクセス許可鍵記憶手段に格納されたアクセス許可鍵と該アクセス許可鍵群記憶手段に格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手段と、

通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手段と、

を備え、

該認証情報生成手段は、

該セキュア領域に格納されている媒体固有の媒体IDを該相互認証を行った上で読み出し、該主ファイル認証情報および該副ファイル認証情報の生成に使用することを特徴とするファイル管理システム。

【請求項21】 請求項20に記載のファイル管理システムであって、

前記計算機に備えられた相互認証手段および前記ファイルアクセス手段は、ハードウェアで実現されることを特徴とするファイル管理システム。

【請求項22】 請求項20または21に記載のファイル管理システムであって、

50 該媒体IDは、カードIDであることを特徴とするファ

イル管理システム。

【請求項23】 請求項20または21に記載のファイル管理システムであって、

該媒体IDは、マスタIDであることを特徴とするファイル管理システム。

【請求項24】 請求項20～23のいずれか1項記載のファイル管理システムであって、

前記認証情報の生成は、ファイルのレコードごとに行うことを特徴とするファイル管理システム。

【請求項25】 請求項1記載のファイル管理システムであって、

前記セキュア領域アクセス手段は、

前記セキュア領域に格納されたアクセス制御情報を読み出すアクセス制御情報読出手段と、

を更に備え、

前記記憶装置は、該アクセス制御情報に従い主ファイルまたは該主ファイルと関連付けられた副ファイルに対しセクタあるいはセクタ群単位でアクセスするセクタアクセス手段と、をさらに備えることを特徴とするファイル管理システム。

【請求項26】 請求項25記載のファイル管理システムであって、

前記セキュア領域アクセス手段は、

前記セキュア領域にアクセス制御情報を設定するアクセス制御情報設定手段をさらに備えることを特徴とするファイル管理システム。

【請求項27】 請求項9～13、20～24のいずれか1項記載のファイル管理システムであって、前記媒体IDまたは前記カードIDまたは前記マスタIDのうち、1つまたは2つまたは3つのIDを用いて認証情報を生成することを特徴とするファイル管理システム。

【請求項28】 計算機と記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証工程と、

該アクセス許可鍵を格納するアクセス許可鍵記憶工程と、

該アクセス許可鍵を格納するアクセス許可鍵群記憶工程と、

該アクセス許可鍵とともにアクセス要求を送付するファイルアクセス工程と、

該アクセス許可鍵記憶工程で格納されたアクセス許可鍵と該アクセス許可鍵群記憶工程で格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別工程と、

通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス工程と、

を備えたファイル管理方法。

【請求項29】 計算機と記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手順と、

該アクセス許可鍵を格納するアクセス許可鍵記憶手順と、

該アクセス許可鍵を格納するアクセス許可鍵群記憶手順と、

該アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手順と、該アクセス許可鍵記憶手順で格納されたアクセス許可鍵と該アクセス許可鍵群記憶手順で格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手順と、

通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手順と、

を備えた機能をコンピュータに実現させるためのファイル管理プログラムを記録したコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ファイルの改ざん防止および検出機能を有するファイル管理システムに関し、特に、データファイルから間接的に生成した認証子を、操作者がアクセスできない領域に格納することで、ファイルの改ざん防止および検出を可能とするファイル管理システムに関する。

【0002】

【従来の技術】税務関連帳票等の公文書の電子化が進むにつれ、紙で保存していた時と同様に電子化データを長期間、安全に、証拠能力を保って保存したいというニーズが高まっている。電子化データは、追加、削除、修正あるいはネットワークなどを介しての転送など、加工や再利用が非常に容易である。このため、電子化データは、作成者が作成した通りのものではなく、第三者がデータを改ざんする危険性がある。

【0003】この問題を解決するため、出願人は、特願平9-88485号（ファイルシステムおよびプログラム記録媒体、平成9年4月7日出願）を出願した。これは、OS（Operating System）内のファイル管理モジュール（ファイルシステム）と、ユーザには通常アクセスを許さない領域（セキュア領域）を設定できる記憶媒体（セキュア媒体）が連携して、セキュア領域にデータファイルの改ざん検出用の認証子およびデータファイルのアクセスログ等をデータファイルに関連付けて保存しておくことで、不正ユーザの低レベルアクセスによる不正改ざんの検出、また正当ユーザの悪意を持った不正改ざんの検出が行えるファイルシステムである。

【0004】

【発明が解決しようとする課題】ところが、上記従来例では、通常ユーザによるセキュア領域アクセスをファイルシステムにより守っているため、そのようなファイルシステムを有さないシステムでは容易にセキュア領域がアクセスされ、その結果データファイルに関連付けられた認証子、アクセスログ等が都合のいいように改ざんさ

れてしまう可能性があった。

【0005】また、アクセスログ等は動的に拡大するため、アクセスの頻度等によって必要なセキュア領域のサイズは異なるが、一般的にセキュア領域と通常の領域のサイズを動的に変更することは難しい。

【0006】

【課題を解決するための手段】そこで、本発明では、上記従来例の前者の問題に対してはセキュア領域をファイルシステムではなく、ファイルシステムとの間で相互認証の得られた記憶装置の例えばファームウェアで守るという方法をとることで問題を解決する。また、後者の問題に対しては、主ファイルであるデータファイルに関連付けられた認証子やアクセスログ等の副ファイルは通常の領域に置き、上記副ファイルから生成した認証子だけをセキュア領域に置くことで問題解決をはかる。請求項1の発明は、計算機と記憶装置とを備えたファイルシステムであって、上記計算機は、上記記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、上記アクセス許可鍵を格納するアクセス許可鍵記憶手段と、上記アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手段と、を備え、上記記憶装置は、上記計算機との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、上記アクセス許可鍵を格納するアクセス許可鍵群記憶手段と、上記アクセス許可鍵記憶手段に格納されたアクセス許可鍵と上記アクセス許可鍵群記憶手段に格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手段と、通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手段と、を備えたファイル管理システムである。

【0007】請求項2の発明は、請求項1に記載のファイル管理システムであって、上記計算機に備えられた相互認証手段および上記ファイルアクセス手段は、ハードウェアで実現されることを特徴とするファイル管理システムである。

【0008】請求項3の発明は、主ファイルに関連付けられた一つまたは複数の副ファイルを格納する副ファイル格納手段と、上記副ファイルの検証に使用する副ファイル認証情報を生成する認証情報生成手段と、上記副ファイル認証情報をシステムファイルとして関連付けて格納するシステムファイル格納手段と、を備えることを特徴とするファイル管理システムである。

【0009】請求項4の発明は、主ファイルを格納する主ファイル格納手段と、上記主ファイルの検証に使用する主ファイル認証情報を生成する認証情報生成手段と、上記主ファイル認証情報を副ファイルの1つとして関連付けて格納する副ファイル格納手段と、を備えることを特徴とするファイル管理システムである。

【0010】請求項5の発明は、主ファイルを格納する主ファイル格納手段と、上記主ファイルの検証に使用する

る主ファイル認証情報を生成する認証情報生成手段と、上記主ファイル認証情報を副ファイルの1つとして関連付けて格納する副ファイル格納手段と、主ファイルに関連付けられた一つまたは複数の副ファイルを格納する副ファイル格納手段と、上記副ファイルの検証に使用する副ファイル認証情報を生成する認証情報生成手段と、上記副ファイル認証情報をシステムファイルとして関連付けて格納するシステムファイル格納手段と、を備えることを特徴とするファイル管理システムである。

10 【0011】請求項6の発明は、請求項5において、上記主ファイル、上記副ファイルおよび上記システムファイルを通常アクセスできる非セキュア領域に格納することを特徴とするファイル管理システムである。

【0012】請求項7の発明は、請求項5において、上記主ファイルを通常アクセスできる非セキュア領域に格納し、上記副ファイルおよび上記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システムである。

20 【0013】請求項8の発明は、請求項5において、上記主ファイルおよび上記副ファイルを通常アクセスできる非セキュア領域に格納し、上記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システムである。

【0014】請求項9の発明は、請求項6～8のいずれか1項記載のファイル管理システムであって、計算機と、記憶装置とを更に備え、上記計算機は、上記記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、上記アクセス許可鍵を格納するアクセス許可鍵記憶手段と、上記アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手段と、を備え、上記記憶装置は、上記計算機との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、上記アクセス許可鍵を格納するアクセス許可鍵群記憶手段と、上記アクセス許可鍵記憶手段に格納されたアクセス許可鍵と上記アクセス許可鍵群記憶手段に格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手段と、通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手段と、を備え、上記認証情報生成手段

40 は、上記セキュア領域に格納されている媒体固有の媒体IDを上記相互認証を行った上で読み出し、上記主ファイル認証情報および上記副ファイル認証情報の生成に使用することを特徴とするファイル管理システムである。

【0015】請求項10の発明は、請求項9に記載のファイル管理システムであって、上記計算機に備えられた相互認証手段および上記ファイルアクセス手段は、ハードウェアで実現されることを特徴とするファイル管理システムである。

50 【0016】請求項11の発明は、請求項9または10に記載のファイル管理システムであって、上記媒体ID

は、カードIDであることを特徴とするファイル管理システムである。

【0017】請求項12の発明は、請求項9または10に記載のファイル管理システムであって、上記媒体IDは、マスタIDであることを特徴とするファイル管理システムである。

【0018】請求項13の発明は、請求項9～12のいずれか1項記載のファイル管理システムであって、上記認証情報の生成は、ファイルのレコードごとに行うことを特徴とするファイル管理システムである。

【0019】請求項14の発明は、主ファイルに関連付けられた1つまたは複数の副ファイルを読み出す副ファイル読出手段と、上記副ファイル読出手段から読み出された副ファイルから副ファイル認証情報を生成する認証情報生成手段と、上記副ファイルに関連付けられたシステムファイルから副ファイル認証情報を読み出すシステムファイル読出手段と、上記認証情報生成手段生成した副ファイル認証情報と上記システムファイル読出手段が読み出した副ファイル認証情報とを比較する認証情報比較手段と、備えることを特徴とするファイル管理システムである。

【0020】請求項15の発明は、主ファイルを読み出す主ファイル読出手段と、上記主ファイル読出手段から読み出された主ファイルから主ファイル認証情報を生成する認証情報生成手段と、上記主ファイルに関連付けられた副ファイルから主ファイル認証情報を読み出す副ファイル読出手段と、上記認証情報生成手段生成した主ファイル認証情報と上記副ファイル読出手段が読み出した主ファイル認証情報とを比較する認証情報比較手段と、備えることを特徴とするファイル管理システムである。

【0021】請求項16の発明は、主ファイルを読み出す主ファイル読出手段と、上記主ファイルに関連付けられた1つまたは複数の副ファイルおよび上記主ファイルに関連付けられた副ファイルから主ファイル認証情報を読み出す副ファイル読出手段と、上記副ファイルに関連付けられたシステムファイルから副ファイル認証情報を読み出すシステムファイル読出手段と、上記主ファイル読出手段から読み出された主ファイルから主ファイル認証情報を生成し、上記副ファイル読出手段から読み出された副ファイルから副ファイル認証情報を生成する認証情報生成手段と、上記認証情報生成手段生成した主ファイル認証情報と上記副ファイル読出手段が読み出した主ファイル認証情報とを比較し、上記認証情報生成手段生成した副ファイル認証情報と上記システムファイル読出手段が読み出した副ファイル認証情報とを比較する認証情報比較手段と、備えることを特徴とするファイル管理システムである。

【0022】請求項17の発明は、請求項16において、上記主ファイル、上記副ファイルおよび上記システムファイルを通常アクセスできる非セキュア領域に格納

することを特徴とするファイル管理システムである。

【0023】請求項18の発明は、請求項16において、上記主ファイルを通常アクセスできる非セキュア領域に格納し、上記副ファイルおよび上記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システムである。

【0024】請求項19の発明は、請求項16において、上記主ファイルおよび上記副ファイルを通常アクセスできる非セキュア領域に格納し、上記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システムである。

【0025】請求項20の発明は、請求項17～19のいずれか1項記載のファイル管理システムであって、計算機と、記憶装置とを更に備え、上記計算機は、上記記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、上記アクセス許可鍵を格納するアクセス許可鍵記憶手段と、上記アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手段と、を備え、上記記憶装置は、上記計算機との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、上記アクセス許可鍵を格納するアクセス許可鍵群記憶手段と、上記アクセス許可鍵記憶手段に格納されたアクセス許可鍵と上記アクセス許可鍵群記憶手段に格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手段と、通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手段と、を備え、上記認証情報生成手段は、上記セキュア領域に格納されている媒体固有の媒体IDを上記相互認証を行った上で読み出し、上記主ファイル認証情報および上記副ファイル認証情報の生成に使用することを特徴とするファイル管理システムである。

【0026】請求項21の発明は、請求項20に記載のファイル管理システムであって、上記計算機に備えられた相互認証手段および上記ファイルアクセス手段は、ハードウェアで実現されることを特徴とするファイル管理システムである。

【0027】請求項22の発明は、請求項20または21に記載のファイル管理システムであって、上記媒体IDは、カードIDであることを特徴とするファイル管理システムである。

【0028】請求項23の発明は、請求項20または21に記載のファイル管理システムであって、上記媒体IDは、マスタIDであることを特徴とするファイル管理システムである。

【0029】請求項24の発明は、請求項20～23のいずれか1項記載のファイル管理システムであって、上記認証情報の生成は、ファイルのレコードごとに行うことを特徴とするファイル管理システムである。

【0030】請求項25の発明は、請求項1記載のファ

イル管理システムであって、上記記憶装置は、主ファイルまたは上記主ファイルと関連付けられた副ファイルに対しセクタあるいはセクタ群単位でアクセスするセクタアクセス手段とをさらに備え、上記セキュア領域アクセス手段は、上記セキュア領域に格納されたアクセス制御情報を読み出すアクセス制御情報読出手段と、を備えることを特徴とするファイル管理システムである。

【0031】請求項26の発明は、請求項25記載のファイル管理システムであって、上記セキュア領域アクセス手段は、上記セキュア領域にアクセス制御情報を設定するアクセス制御情報設定手段をさらに備えることを特徴とするファイル管理システムである。

【0032】請求項27の発明は、請求項9～13、20～24のいずれか1項記載のファイル管理システムであって、上記媒体1Dまたは上記カード1Dまたは上記マスタ1Dのうち、1つまたは2つまたは3つの1Dを用いて認証情報を生成することを特徴とするファイル管理システムである。

【0033】請求項28の発明は、計算機と記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証工程と、上記アクセス許可鍵を格納するアクセス許可鍵記憶工程と、上記アクセス許可鍵とともにアクセス要求を送付するファイルアクセス工程と、上記アクセス許可鍵を格納するアクセス許可鍵群記憶工程と、上記アクセス許可鍵記憶工程で格納されたアクセス許可鍵と上記アクセス許可鍵群記憶工程で格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別工程と、通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス工程と、を備えたファイル管理方法である。

【0034】請求項29の発明は、計算機と記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手順と、上記アクセス許可鍵を格納するアクセス許可鍵記憶手順と、上記アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手順と、上記アクセス許可鍵を格納するアクセス許可鍵群記憶手順と、上記アクセス許可鍵記憶手順で格納されたアクセス許可鍵と上記アクセス許可鍵群記憶手順で格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手順と、通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手順と、を備えた機能をコンピュータに実現させるためのファイル管理プログラムを記録したコンピュータ読取り可能な記録媒体である。

【0035】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態について詳細に説明する。図1は、本発明の実施の形態における改ざん防止／検出機能を有するファイル管理システムの全体構成図である。

【0036】各構成部は、図4、図6、図8、図10、

図12、図14、図15、図16、図18、図20、図22、図24、図25、図26、図28、および図30を用いて各実施の形態を説明しながら後述する。

【0037】なお、計算機1側の相互認証部11、認証情報生成部14および認証情報比較部15等の各構成部は、それぞれ、OS内のファイル管理モジュール内におけるソフトウェアサブルーチンであっても良いし、ハードウェアにより構成されていても良い。

【0038】図2は、本発明の実施の形態におけるファイルの構成を説明するための図である。主ファイルから生成された認証子は副ファイルに格納され、副ファイルから生成された認証子はシステムファイルに格納される。

【0039】図3は、MACの計算方法を説明するための図である。主ファイルや副ファイルなどの元データを例えば64bitずつに分割し、暗号化する。暗号化された値と次の64bitとの排他的論理和をとり、これをまた暗号化する。それぞれの暗号化により得られた値あるいはその値のうちの一部、例えば上位32bitを認証子とする事もできるが、後述する各実施の形態においては、この処理を最後まで繰り返し、最終的に得られた値の上位32bitを認証子とする。

【0040】図4は、本発明の第1の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図5は、本発明の第1の実施の形態における動作フローチャートである。

【0041】ステップS51で、計算機1側の相互認証部11と記憶装置2側の相互認証部21は、計算機1および記憶装置2の双方の間で相互認証を行う。ステップS52で、相互認証に成功したら、ステップ53で、共通のアクセス許可鍵を生成する。ステップS54で、計算機1側の相互認証部11は、生成したアクセス許可鍵をアクセス許可鍵記憶部12に渡し格納する。また、記憶装置2側の相互認証部21は、生成したアクセス許可鍵をアクセス許可鍵群記憶部22に渡し格納する。相互認証の方法は、例えば一般的な公開鍵を用いたものにする。

【0042】ステップS55で、ファイルアクセス部13は、記憶装置2を介してアクセスする媒体3上のセキュア領域31にアクセスする場合に、記憶装置2のセキュア領域アクセス部24に対し、アクセス要求とともにアクセス許可鍵を送付する。

【0043】ステップS56で、アクセス許可鍵判別部23は、セキュア領域アクセス部24に対するファイルアクセス部13からのアクセス要求とともに送付されたアクセス許可鍵と同一のアクセス許可鍵が、アクセス許可鍵記憶部22内に存在するかどうかを判別する。存在すれば、ステップS57で、セキュア領域アクセス部24は、セキュア領域31へのアクセスを行う。

【0044】なお、計算機1側の相互認証部11およびファイルアクセス部13は、それぞれ、OS内のファイ

ル管理モジュール内におけるソフトウェアサブルーチンであっても良いし、ハードウェアにより構成されていても良い。

【0045】図6は、本発明の第2の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図7は、本発明の第2の実施の形態における動作フローチャートである。

【0046】ステップS71で、副ファイル格納部138は、媒体3に副ファイル34をブロック単位に格納するとともに、後述するステップS74の処理から戻ってきた場合、すなわち、他に副ファイル34が存在すれば読み出し、今格納しようとしている副ファイル34と結合して認証情報生成部14に渡す。

【0047】ステップS72で、認証情報生成部14は、結合された副ファイル群34から認証情報である認証子を生成し、システムファイル格納部134に渡す。ステップS73で、副ファイル34の終端に達したかどうかを見て、終端に達していなければ、ステップS71に戻り、副ファイル34の次のブロックを処理する。

【0048】ステップS73で、複数ある副ファイル34の全ての副ファイル34について処理したかどうかを見て、処理していない副ファイル34があれば、ステップS71に戻り、次の副ファイル34を処理する。

【0049】ステップS74で、システムファイル格納部134は、主ファイル33および副ファイル群34を一意に識別できるなんらかのIDと認証情報である認証子とをセットにして、システムファイル35中に格納する。

【0050】図8は、本発明の第3の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図9は、本発明の第3の実施の形態における動作フローチャートである。

【0051】ステップ91で、主ファイル格納部136は、媒体3に主ファイル33をブロック単位に格納するとともに、主ファイル33を認証情報生成部14にも渡す。ステップ92で、これを受け取った認証情報生成部14は、認証情報である認証子を生成し、副ファイル格納部138に渡す。ステップS93で、主ファイル33の終端に達したかどうかを見て、終端に達していなければ、ステップS91に戻り、主ファイル33の次のブロックを処理する。

【0052】ステップS94で、副ファイル格納部138は、主ファイル33を一意に識別できるなんらかのIDと認証情報である認証子とをセットにし特定の副ファイル34中に格納する。図10は、本発明の第4の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図11は、本発明の第4の実施の形態における動作フローチャートである。

【0053】ステップS111で、主ファイル格納部136は、媒体3に主ファイル33をブロック単位に格納

を行うとともに、認証情報生成部14に主ファイル33を渡す。

【0054】ステップS112で、認証情報生成部14は、主ファイル33から認証情報である認証子を生成し、副ファイル格納部138に渡す。ステップS113で、主ファイル33の終端に達したかどうかを見て、終端に達していなければ、ステップS111に戻り、主ファイル33の次のブロックを処理する。

【0055】ステップS114で、副ファイル格納部138は、主ファイル33を一意に識別できるなんらかのIDと認証情報である認証子とをセットし、特定の副ファイル34に格納する。

【0056】次に、ステップ115で、副ファイル読出部139は、副ファイル群34を読み出し、認証情報生成部14に渡す。ステップ116で、認証情報生成部14は、認証情報である認証子を生成し、システムファイル格納部134に渡す。ステップS117で、副ファイル34の終端に達したかどうかを見て、終端に達していなければ、ステップS115に戻り、副ファイル34の次のブロックを処理する。

【0057】ステップS118で、複数ある副ファイル34の全ての副ファイル34について処理したかどうかを見て、処理していない副ファイル34があれば、ステップS115に戻り、次の副ファイル34を処理する。全副ファイルの処理が実行される事により、副ファイル読出部139は、副ファイル群34をすべて読み出し、認証情報生成部14に渡したことになる。

【0058】ステップS119で、システムファイル格納部134は、主ファイル33および副ファイル34を一意に識別できるなんらかのIDと認証情報である認証子とをセットにして、システムファイル35に格納する。なお、主ファイル33は、非セキュア領域32に格納されているが、副ファイル34およびシステムファイル35は、セキュア領域31に格納されていても非セキュア領域32に格納されていても良い。つまり、実データである主ファイル33は、通常アクセスできる非セキュア領域32に格納されている必要があり、直接アクセスする必要のない副ファイル34およびシステムファイル35は、直接的にはアクセスしないので、セキュア領域31に格納されていても非セキュア領域32に格納されていても良い。

【0059】図12は、本発明の第5の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図13は、本発明の第5の実施の形態における動作フローチャートである。

【0060】第1の実施の形態で説明した相互認証は、予め行っておく。ステップ130で、媒体ID読出部16は、媒体3上のセキュア領域31から媒体ID36を読み出し、認証情報生成部14に渡す。

【0061】ステップ131で、主ファイル格納部13

6は、媒体3に主ファイル33をブロック単位に格納するとともに、認証情報生成部14にも主ファイル33を渡す。

【0062】ステップ132で、認証情報生成部14は、渡された主ファイル33から媒体ID36を鍵として認証情報である認証子を生成し、副ファイル格納格納部138に渡す。ここではDES-MACを使用し認証子を生成することにする。

【0063】ステップS133で、主ファイル33の終端に達したかどうかを見て、終端に達していなければ、ステップS131に戻り、主ファイル33の次のブロックを処理する。

【0064】ステップS134で、副ファイル格納部138は、主ファイル33を一意に識別できるなんらかのIDと認証情報である認証子とをセットにして、特定の副ファイル34中に格納する。

【0065】次に、ステップS135で、副ファイル読出部139は、副ファイルを読み出し、認証情報生成部14に渡す、さらに、後述するステップS138の処理から戻ってきた場合、上述のステップS134で格納したデータを結合し認証情報生成部14に渡す。すなわち、副ファイル群34をすべて読み出し、今格納した全てを結合し認証情報生成部14に渡すことになる。

【0066】ステップS136で、認証情報生成部14は、上述と同様に認証情報である認証子を生成し、システムファイル格納部134に渡す。ステップS137で、副ファイル34の終端に達したかどうかを見て、終端に達していなければ、ステップS135に戻り、副ファイル34の次のブロックを処理する。

【0067】ステップS138で、複数ある副ファイル34の全ての副ファイル34について処理したかどうかを見て、処理していない副ファイル34があれば、ステップS135に戻り、次の副ファイル34を処理する。

【0068】ステップS139で、システムファイル格納部134は、主ファイル33および副ファイル群34を一意に識別できるなんらかのIDと認証情報をセットにし、システムファイル35中に格納する。

【0069】なお、認証子生成時の鍵として用いる媒体ID36は、予め媒体3より読み込んでおいても良い。さらに、主ファイル33および副ファイル34は、これらを構成するレコードごとに、上述のような処理を行っても良い。

【0070】図14は、本発明の第6の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図12を用いて説明した第5の実施の形態における媒体ID読出部16が読み出す媒体ID36が、カードID18に代わっているだけで、その他の構成および基本的な動作は同じである。

【0071】図15は、本発明の第7の実施の形態における改ざん防止／検出機能を有するファイル管理システ

ムの構成図である。図12を用いて説明した第5の実施の形態における媒体ID読出部16が読み出す媒体ID36が、複数のハードウェアで共通であるマスタID17に代わっているだけで、その他の構成および基本的な動作は同じである。

【0072】図16は、本発明の第8の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図17は、本発明の第8の実施の形態における動作フローチャートである。

【0073】ステップS171で、上位層（ユーザ等）から入出力部41を介して検証要求が発生した場合、システムファイル読出部135は、システムファイル35中より対応する認証情報である認証子を読み出し、認証情報比較部15に渡す。

【0074】一方、ステップS172で、副ファイル読出部139は、副ファイル34をブロック単位に読み出し、認証情報生成部14に渡す。ステップS173で、認証情報生成部14は、認証情報である認証子を生成し、認証情報比較部15に渡す。

【0075】ステップS174で、副ファイル34の終端に達したかどうかを見て、終端に達していなければ、ステップS172に戻り、副ファイル34の次のブロックを処理する。

【0076】ステップS175で、複数ある副ファイル34の全ての副ファイル34について処理したかどうかを見て、処理していない副ファイル34があれば、ステップS172に戻り、次の副ファイル34を処理する。

【0077】ステップS176で、認証情報比較部15は、これらの認証情報である認証子と比較し、同じであれば検証成功、同じでなければ検証失敗を上位層に通知する。

【0078】図18は、本発明の第9の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図19は、本発明の第9の実施の形態における動作フローチャートである。

【0079】ステップS191で、上位層（ユーザ等）から入出力部41を介して検証要求が発生した場合、副ファイル読出部139は、特定の副ファイル34中より対応する認証情報である認証子を読み出し、認証情報比較部15に渡す。

【0080】一方、ステップS192で、主ファイル読出部137は、主ファイル33をブロック単位に読み出し、認証情報生成部14に渡す。ステップS193で、認証情報生成部14は、認証情報である認証子をブロック単位に生成し、認証情報比較部15に渡す。

【0081】ステップS194で、主ファイル33の終端に達したかどうかを見て、終端に達していなければ、ステップS192に戻り、主ファイル33の次のブロックを処理する。

【0082】ステップS195で、認証情報比較部15

10

20

30

40

50

は、これらの認証情報である認証子を比較し、同じであれば検証成功、同じでなければ検証失敗を上位層に通知する。

【0083】図20は、本発明の第10の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図21は、本発明の第10の実施の形態における動作フローチャートである。

【0084】ステップS210で、主ファイル33の読み出し要求が発行されると、まずシステムファイル読出部135が、対応する認証情報である認証子をシステムファイル35から読み出し、認証情報比較部15に渡す。

【0085】一方、ステップS211で、副ファイル読出部139が、副ファイル34ブロック単位に読み出し、認証情報生成部14に渡す。ステップS212で、認証情報生成部14は、これらから認証情報である認証子をブロック単位に再生成し、認証情報比較部15に渡す。

【0086】ステップS213で、副ファイル34の終端に達したかどうかを見て、終端に達していなければ、ステップS211に戻り、副ファイル34の次のブロックを処理する。

【0087】ステップS214で、複数ある副ファイル34の全ての副ファイル34について処理したかどうかを見て、処理していない副ファイル34があれば、ステップS211に戻り、次の副ファイル34を処理する。

【0088】ステップS215で、認証情報比較部15は、これらの認証情報である認証子と再生成した認証情報である認証子とを比較し、同じでなければ検証失敗を上位層に通知する。

【0089】次に、ステップS216で、副ファイル読出部139は、副ファイル34から主ファイル33の認証情報である認証子を読み出し、認証情報比較部15に渡す。

【0090】一方、ステップS217で、主ファイル読出部137は、主ファイル33をブロック単位に読み出し、認証情報生成部14に渡す。ステップS218で、認証情報生成部14は、ブロック単位に認証情報である認証子を再生成し、認証情報比較部15に渡す。

【0091】ステップS219で、主ファイル33の終端に達したかどうかを見て、終端に達していなければ、ステップS217に戻り、主ファイル33の次のブロックを処理する。

【0092】ステップS220で、認証情報比較部15は、読み出した認証情報である認証子と再生成した認証情報である認証子とを比較し、検証結果を上位層に通知する。

【0093】なお、主ファイル33は、非セキュア領域に格納されているが、副ファイル34およびシステムファイル35は、セキュア領域に格納されていても非セキ

ュア領域に格納されていても良い。

【0094】図22は、本発明の第11の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図23は、本発明の第11の実施の形態における動作フローチャートである。

【0095】上位層（ユーザ等）から入出力部41を介して検証要求が発生した場合、ステップS230で、媒体ID読出部16は、媒体3上のセキュア領域31から媒体ID36を読み出し、認証情報生成部14に渡す。

【0096】ステップS231で、システムファイル読出部135は、システムファイル35中より対応する認証情報である認証子を読み出し、認証情報比較部15に渡す。

【0097】ステップS232で、副ファイル読出部139は、副ファイル34をブロック単位に読み出し、認証情報生成部14に渡す。ステップS233で、認証情報生成部14は、媒体ID36を鍵として認証情報である認証子を生成し、認証情報比較部15に渡す。ステップS234で、副ファイル34の終端に達したかどうかを見て、終端に達していなければ、ステップS232に戻り、副ファイル34の次のブロックを処理する。

【0098】ステップS235で、複数ある副ファイル34の全ての副ファイル34について処理したかどうかを見て、処理していない副ファイル34があれば、ステップS232に戻り、次の副ファイル34を処理する。

【0099】ステップS236で、認証情報比較部15は、これらの認証情報である認証子と再生成した認証情報である認証子とを比較し、同じでなければ検証失敗を上位層に通知し、終了する。

【0100】次に、検証に成功した場合、ステップS237で、副ファイル読出部139は、特定の副ファイル34より認証情報である認証子を読み出し、認証情報比較部15に渡す。

【0101】ステップS238で、主ファイル読出部137は、主ファイル33をブロック単位に読み出し、認証情報生成部14に渡す。ステップS239で、認証情報生成部14は、媒体ID36を鍵として認証情報である認証子をブロック単位に生成し、認証情報比較部15に渡す。

【0102】ステップS240で、主ファイル33の終端に達したかどうかを見て、終端に達していなければ、ステップS238に戻り、主ファイル33の次のブロックを処理する。

【0103】ステップS241で、認証情報比較部15は、これらの認証情報である認証子を比較し、同じであれば検証成功を、同じでなければ検証失敗を上位層に通知し、終了する。

【0104】なお、認証子生成時の鍵として用いる媒体ID36は、予め媒体3より読み込んでおいても良い。さらに、主ファイル33および副ファイル34は、これ

らを構成するレコードごとに、上述のような処理を行っても良い。

【0105】図24は、本発明の第12の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図22を用いて説明した第11の実施の形態における媒体ID読出部16が読み出す媒体ID36が、カードID18に代わっているだけで、その他の構成および基本的な動作は同じである。

【0106】図25は、本発明の第13の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図22を用いて説明した第11の実施の形態における媒体ID読出部16が読み出す媒体ID36が、複数のハードウェアで共通であるマスタID17に代わっているだけで、その他の構成および基本的な動作は同じである。

【0107】図26は、本発明の第14の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図27は、本発明の第14の実施の形態における動作フローチャートである。

【0108】ステップS271で、アクセス制御情報設定部242は、アクセス制御情報38を設定あるいは設定の更新をする。設定時のポリシーとしては様々なものが考えられるが、例えば一旦ライト不可能にすると二度とライト可能にはできないというものも考えられる。

【0109】ステップS272で、セキュア領域31に存在するアクセス制御情報38をアクセス制御情報読出部241を通じて読み出し、許可されていないアクセスであれば拒絶を通知する。

【0110】許可されていれば、ステップS273で、セクタアクセス部251は、アクセス（リード／ライト）要求を受け、記憶媒体3上の非セキュア領域32内の主ファイル33および副ファイル34により構成されるセクタ（群）にアクセスする。

【0111】図28は、本発明の第15の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図29は、本発明の第14の実施の形態における動作フローチャートである。

【0112】ステップS291で、アクセス制御情報設定部132は、上位層から指定されたファイルを主副ファイルセクタ群対応表133によりセクタリストに変換し、読み出し専用／書き込み専用／読み書き許可等のアクセスモードと共に記憶装置2内のアクセス制御情報設定部242に送る。

【0113】ステップS292で、記憶装置2内のアクセス制御情報設定部242は、媒体3上に記憶されているアクセス制御情報38とその設定ポリシーに従い、設定あるいは設定を更新する。この時のポリシーとしては、例えば一旦ライト禁止に設定したセクタは二度とライト可能に設定しない等である。

【0114】ステップS293で、主副ファイルアクセ

ス部131は、アクセスしたい主ファイル33および副ファイル34を主副ファイルセクタ群対応表133に従ってセクタ（群）に変換し、セクタアクセス部251に要求を出す。

【0115】ステップS294で、セクタアクセス部251は、アクセス制御情報読出部241を通じて読み出したアクセス制御情報38に従ってセクタアクセスの実行／拒絶を行う。

【0116】図30は、本発明の第16の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図12を用いて説明した第5の実施の形態、図14を用いて説明した第6の実施の形態、図15を用いて説明した第7の実施の形態、図22を用いて説明した第11の実施の形態、図24を用いて説明した第12の実施の形態、および図25を用いて説明した第13の実施の形態における、媒体ID36、カードID18、およびマスタID17のうち、任意の1つまたは2つまたは3つの組み合わせを用いることもできる。

【0117】この際、例えば、媒体ID36の一部にロット番号を現す情報が入っており、特定のロットは長期保存に適した素材、あるいは入念にサーフェスチェックが行われたものであるとする。

【0118】公文書は長期間保存する必要があるため、媒体挿入時にファイルシステムが媒体ID36を読み出し、上記の特定のロットに含まれない媒体である場合に使用できない旨をユーザに通知する。

【0119】なお、本発明の機能が実行されるのであれば、単体の装置であっても、複数の装置からなるシステムあるいは統合装置であっても、LAN等のネットワークを介して処理が行なわれるシステムであっても本発明を適用できることは言うまでもない。

【0120】また、本発明は、図31に示すように、バス319に接続されたCPU311、ROMやRAM312、入力装置313、出力装置314、外部記憶装置315、媒体駆動装置、316、可搬記録媒体319、ネットワーク接続装置317で構成されるシステムでも実現できる。すなわち、前述してきた各実施形態のシステムを実現するソフトウェアのプログラムコードを記録したROMやRAM312、外部記憶装置315、可搬記録媒体319を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPU311やMPU）がプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

【0121】この場合、読み出されたプログラムコード自体が本発明の新規な機能を実現することになり、そのプログラムコードを記録した可搬記録媒体319等は本発明を構成することになる。

【0122】プログラムコードを供給するための可搬記録媒体319としては、例えば、フロッピーディスク、

10

20

30

40

50

ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモリーカード、ROMカード、電子メールやパソコン通信等のネットワーク接続装置 317（言い換えれば、通信回線）を介して記録した種々の記録媒体などを用いることができる。

【0123】また、コンピュータが読み出したプログラムコードを実行することによって、前述した実施形態の機能が実現される他、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているOSなどが実際の処理の一部または全部を行ない、その処理によっても前述した実施形態の機能が実現される。

【0124】さらに、読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリーに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行ない、その処理によっても前述した実施形態の機能が実現される。

【0125】

【発明の効果】以上説明してきたように、本発明は、通常ユーザによるセキュア領域アクセスを記憶装置の例えばファームウェアで守っているため、セキュア領域がアクセスされず、その結果データファイルに関連付けられた認証子、アクセスログ等が改ざんされない。

【0126】また、データファイルに関連付けられた認証子やアクセスログを通常の領域である非セキュア領域に置き、これらの認証子だけをセキュア領域に置くことでセキュア領域のサイズを小さくできる。

【図面の簡単な説明】

【図1】本発明の実施の形態における改ざん防止／検出機能を有するファイル管理システムの全体構成図である。

【図2】本発明の実施の形態におけるファイルの構成を説明するための図である。

【図3】MACの計算方法を説明するための図である。

【図4】本発明の第1の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図5】本発明の第1の実施の形態における動作フローチャートである。

【図6】本発明の第2の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図7】本発明の第2の実施の形態における動作フローチャートである。

【図8】本発明の第3の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図9】本発明の第3の実施の形態における動作フローチャートである。

【図10】本発明の第4の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図11】本発明の第4の実施の形態における動作フローチャートである。

【図12】本発明の第5の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図13】本発明の第5の実施の形態における動作フローチャートである。

【図14】本発明の第6の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図15】本発明の第7の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図16】本発明の第8の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図17】本発明の第8の実施の形態における動作フローチャートである。

【図18】本発明の第9の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図19】本発明の第9の実施の形態における動作フローチャートである。

【図20】本発明の第10の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図21】本発明の第10の実施の形態における動作フローチャートである。

【図22】本発明の第11の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図23】本発明の第11の実施の形態における動作フローチャートである。

【図24】本発明の第12の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図25】本発明の第13の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図26】本発明の第14の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図27】本発明の第14の実施の形態における動作フローチャートである。

【図28】本発明の第15の実施の形態における改ざん

防止／検出機能を有するファイル管理システムの構成図である。

【図29】本発明の第14の実施の形態における動作フローチャートである。

【図30】本発明の第16の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図31】改ざん防止／検出システムの構成図である。

【符号の説明】

- 1 計算機
- 2 記憶装置
- 3 媒体
- 11 相互認証部
- 12 アクセス許可鍵記憶部
- 13 ファイルアクセス部
- 14 認証情報生成部
- 15 認証情報比較部
- 16 媒体ID読出部
- 17 マスタID
- 18 カードID
- 21 相互認証部
- 22 アクセス許可鍵群記憶部
- 23 アクセス許可鍵判別部

- * 24 セキュア領域アクセス部
- 25 非セキュア領域アクセス部
- 31 セキュア領域
- 32 非セキュア領域
- 33 主ファイル
- 34 副ファイル(群)
- 35 システムファイル
- 36 媒体ID
- 38 アクセス制御情報
- 10 41 入出力手段
- 131 主副ファイルアクセス部
- 132 ファイルアクセス制御情報設定部
- 133 主副ファイルセクタ群対応表
- 134 システムファイル格納部
- 135 システムファイル読出部
- 136 主ファイル格納部
- 137 主ファイル読出部
- 138 副ファイル格納部
- 139 副ファイル読出部
- 20 241 アクセス制御情報読出部
- 242 アクセス制御情報設定部
- 251 セクタアクセス部

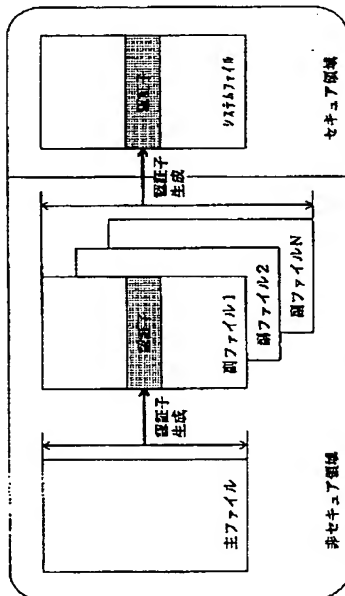
*

【図2】

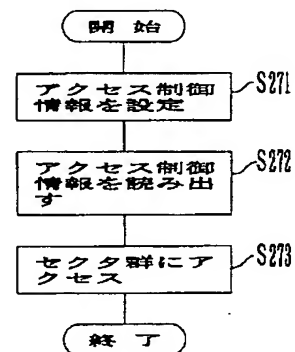
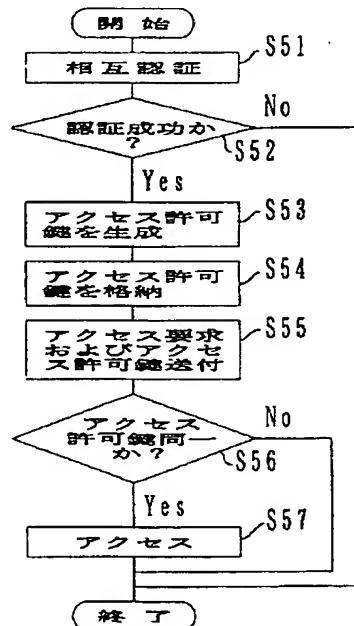
【図5】

【図27】

本発明の実施の形態における
ファイルの構成を説明するため図

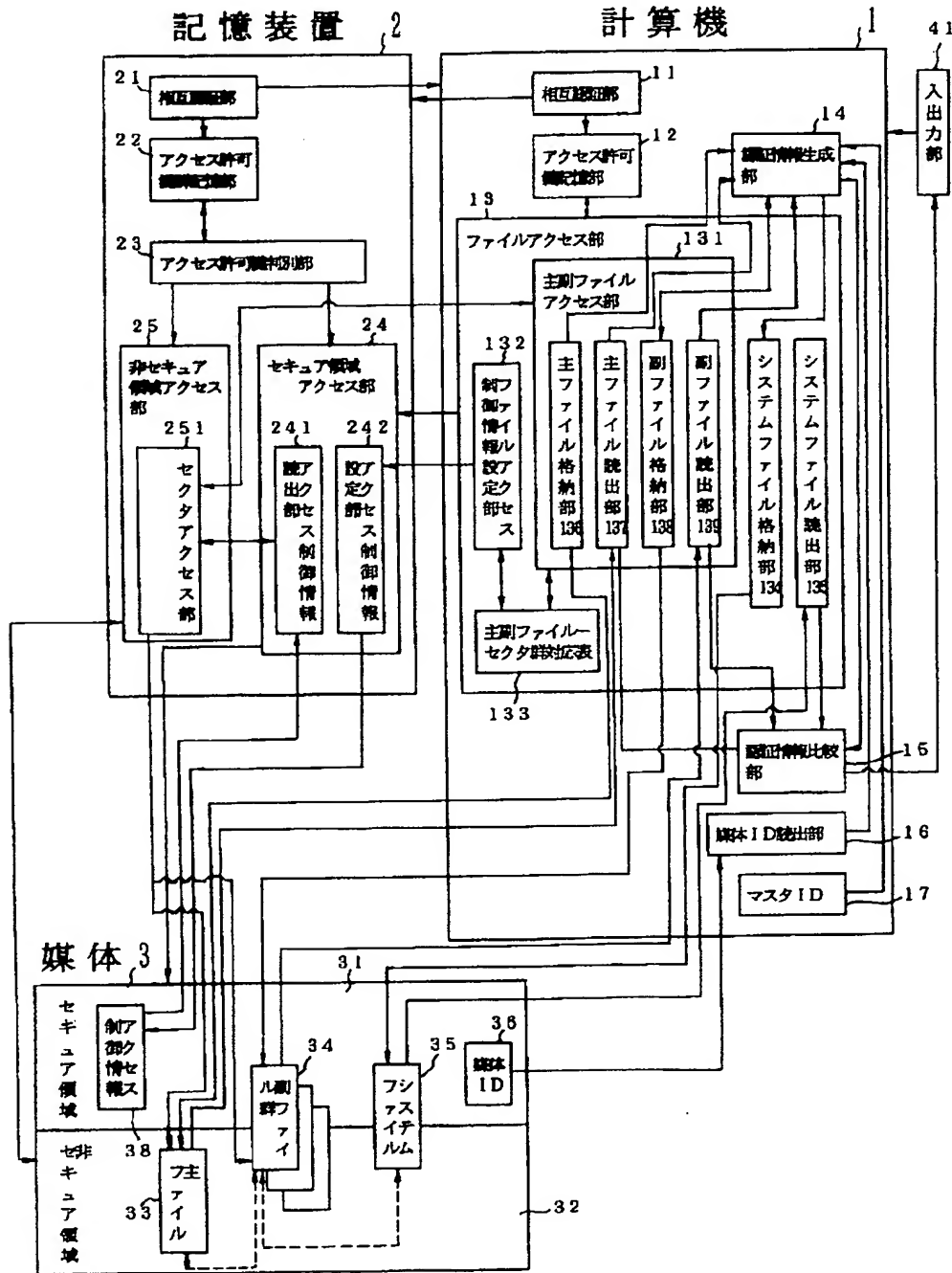


本発明の第1の実施の形態における動作フローチャート 本発明の第14の実施の形態における動作フローチャート



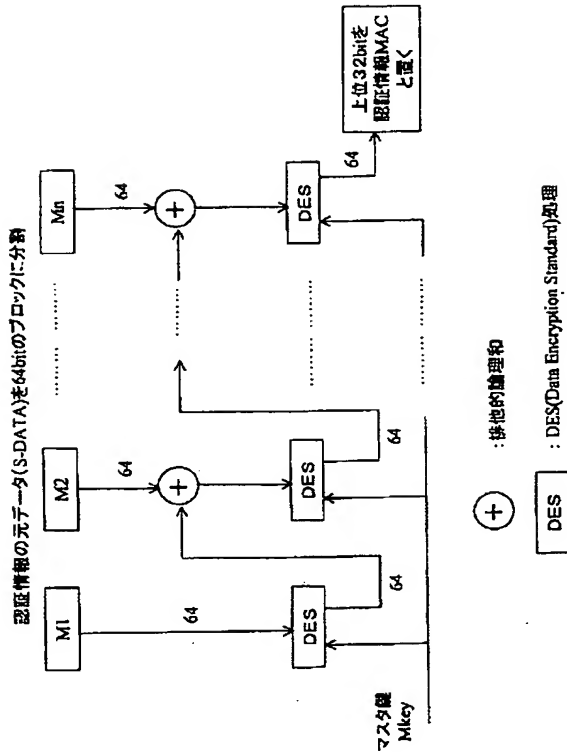
【図1】

本発明の実施の形態における改ざん防止／
検出機能を有するファイル管理システムの全体構成図



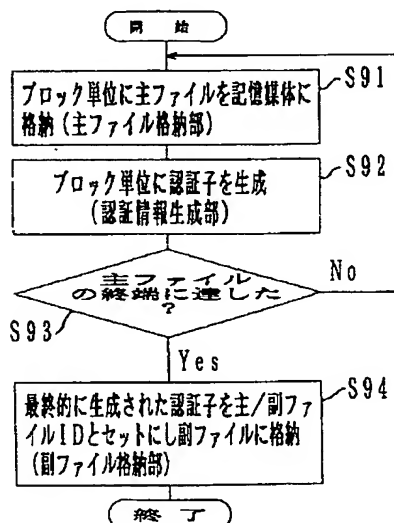
【図3】

MACの計算方法を説明するための図



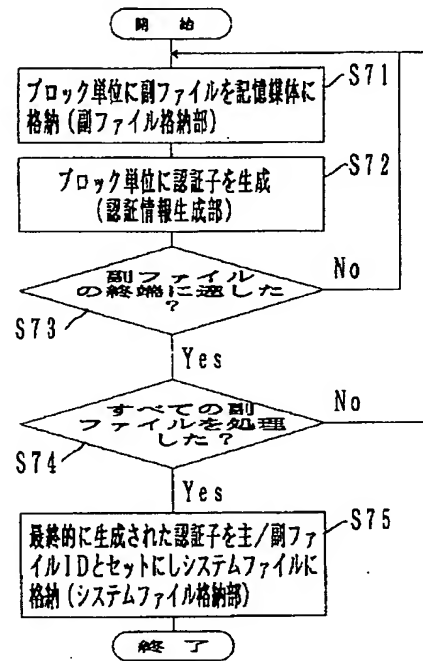
【図9】

本発明の第3の実施の形態における動作フローチャート



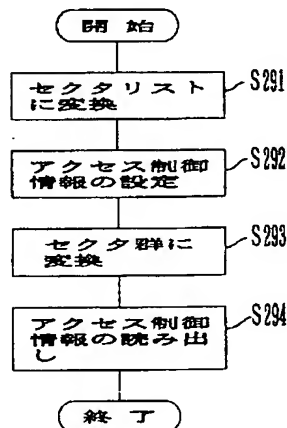
【図7】

本発明の第2の実施の形態における動作フローチャート



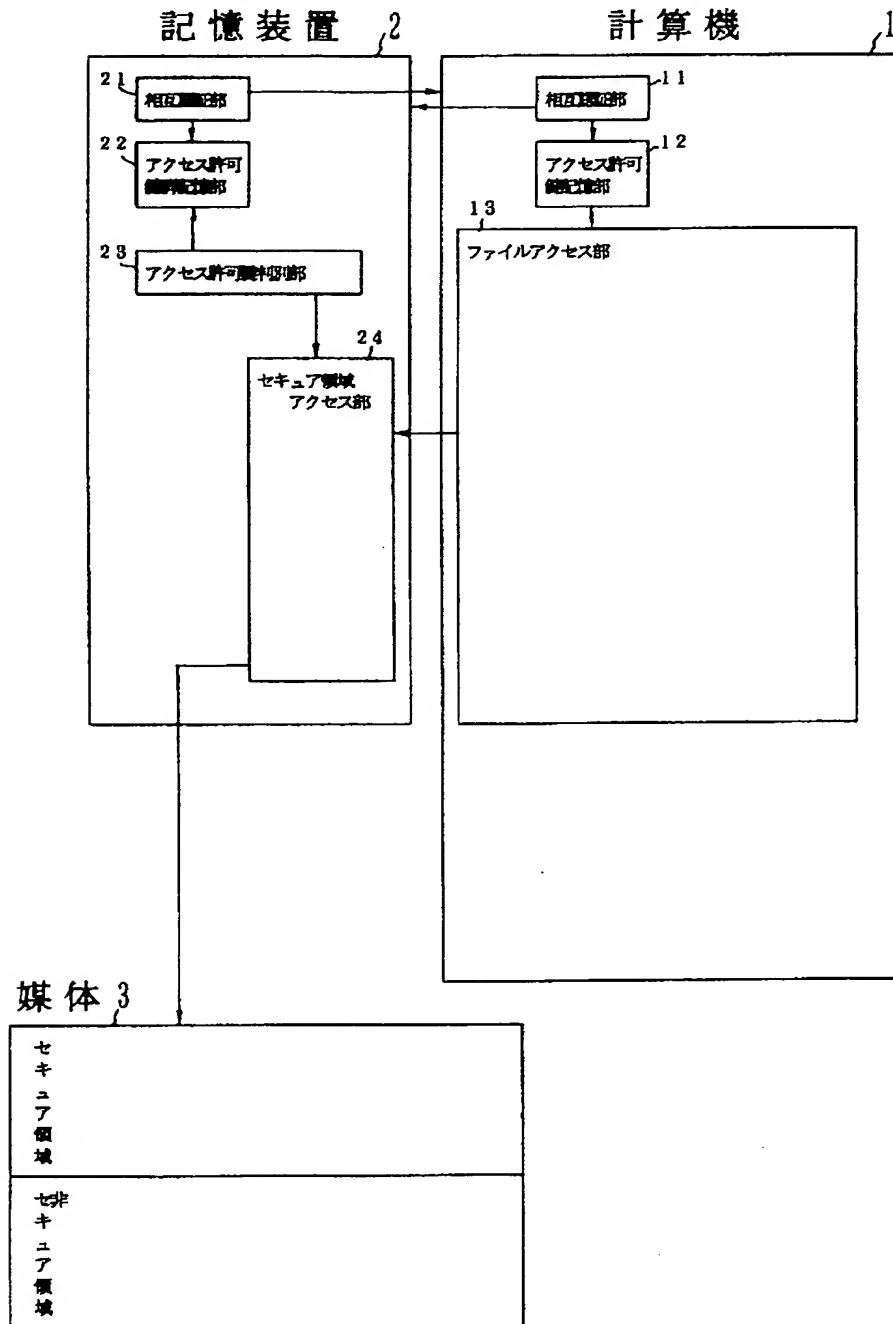
【図29】

本発明の第14の実施の形態における動作フローチャート



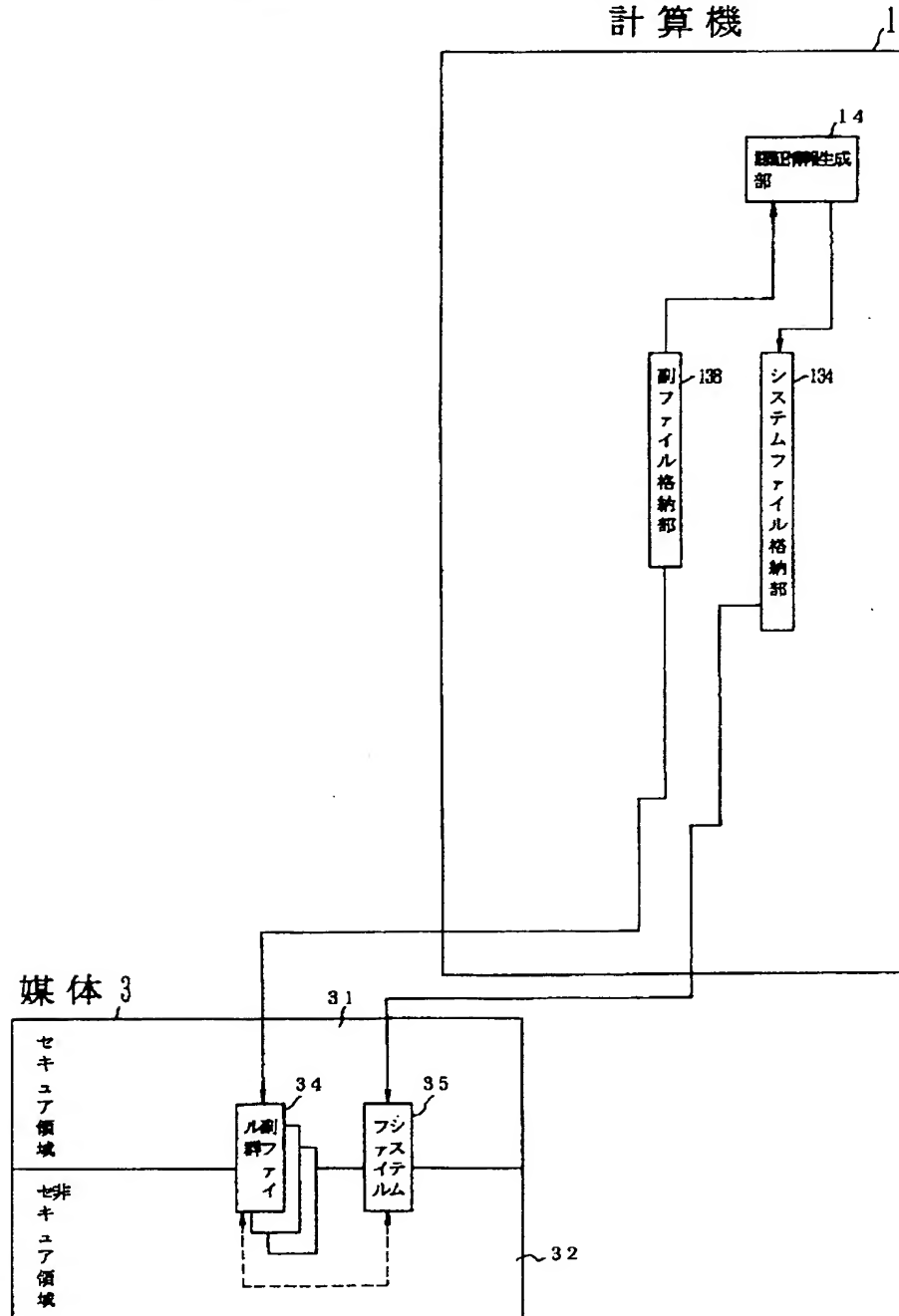
【図4】

本発明の第1の実施の形態における改ざん防止／
検出機能を有するファイル管理システムの構成図



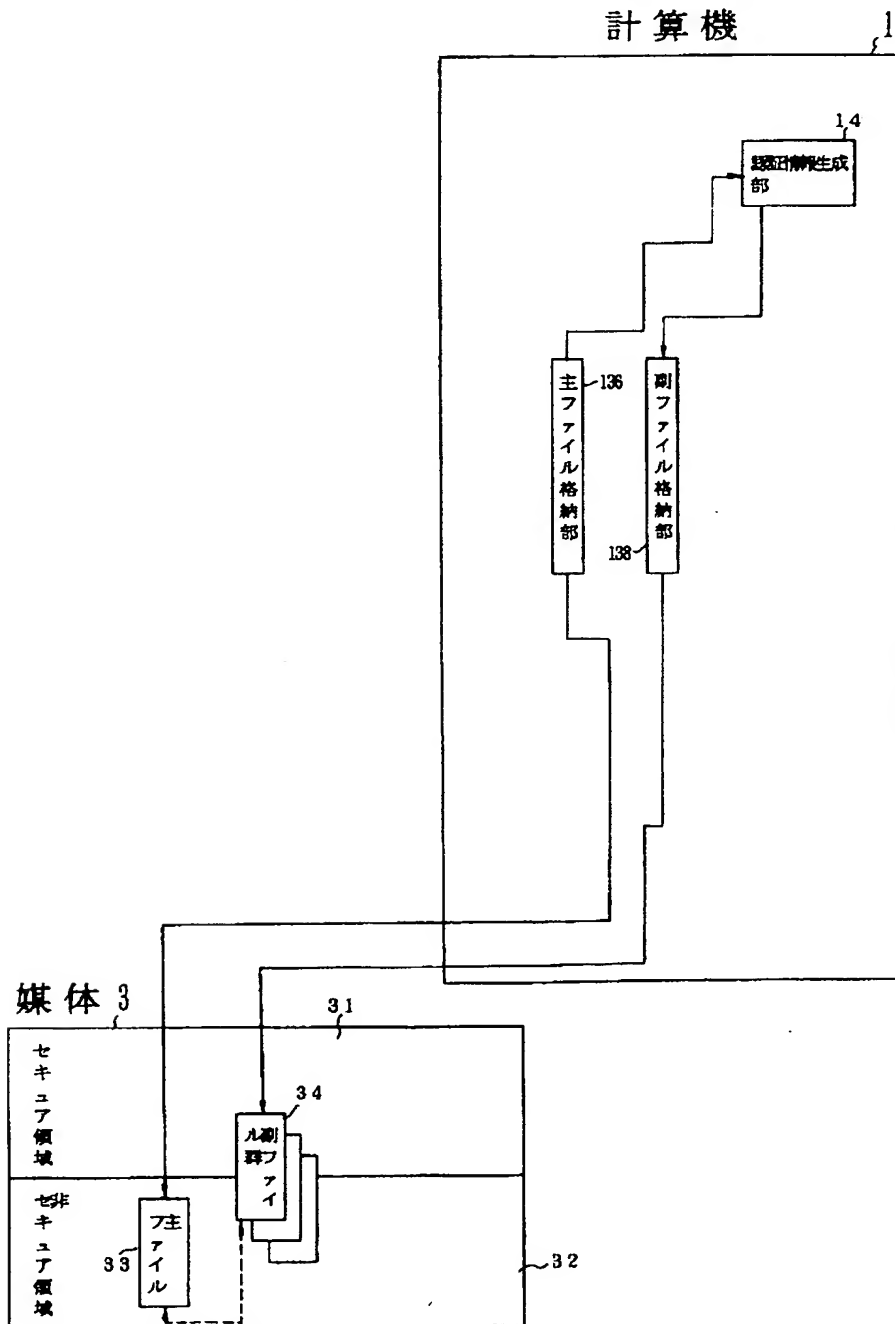
【図6】

本発明の第2の実施の形態における改ざん防止／
検出機能を有するファイル管理システムの構成図



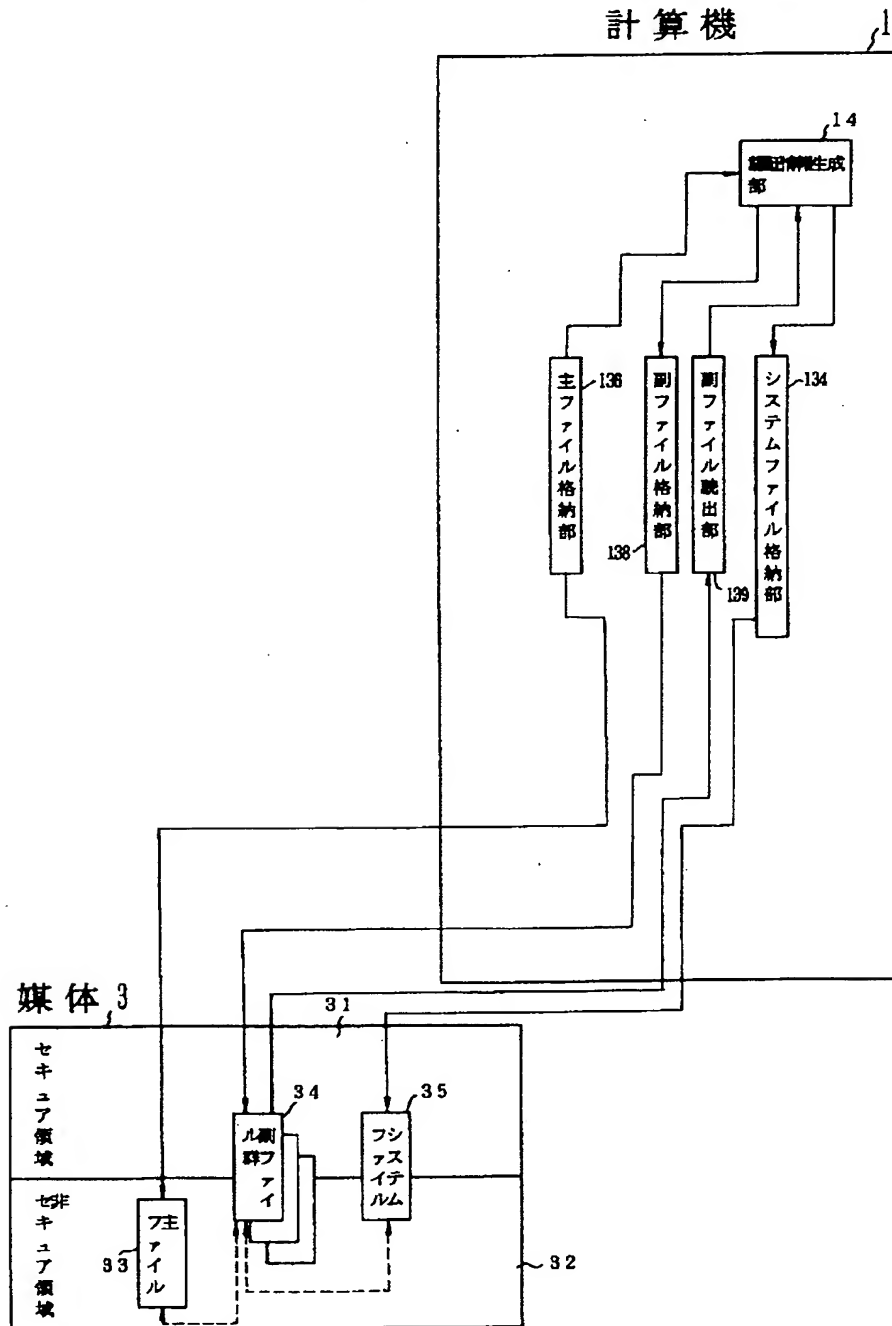
【図8】

本発明の第3の実施の形態における改ざん防止/
検出機能を有するファイル管理システムの構成図



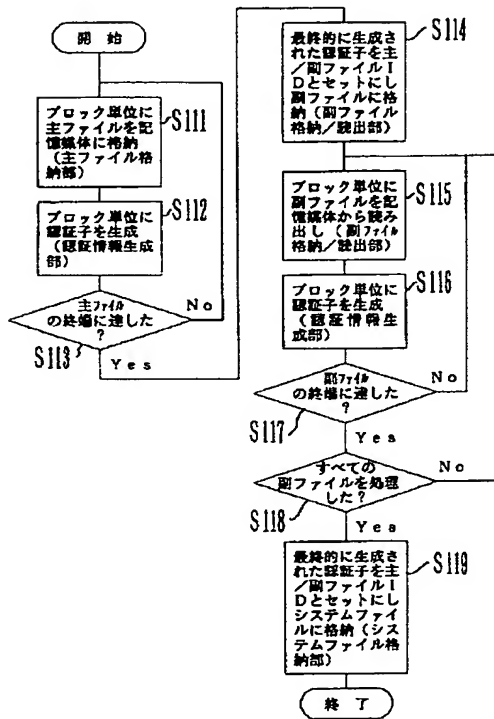
【図10】

本発明の第4の実施の形態における改ざん防止/
検出機能を有するファイル管理システムの構成図



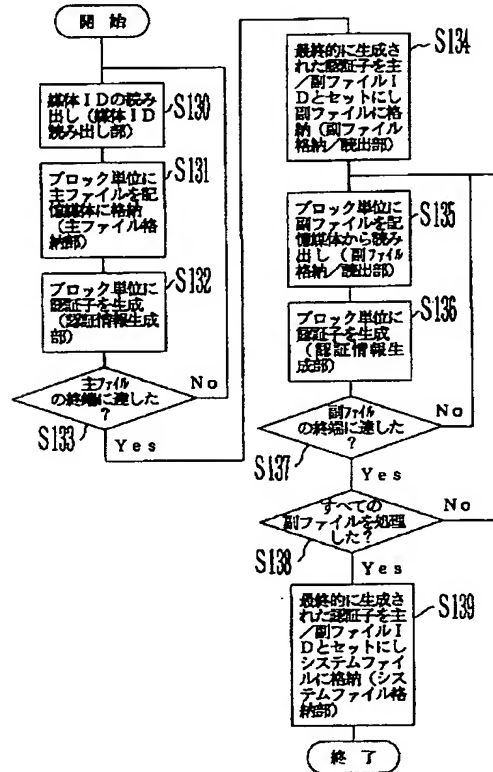
【図11】

本発明の第4の実施の形態における動作フローチャート



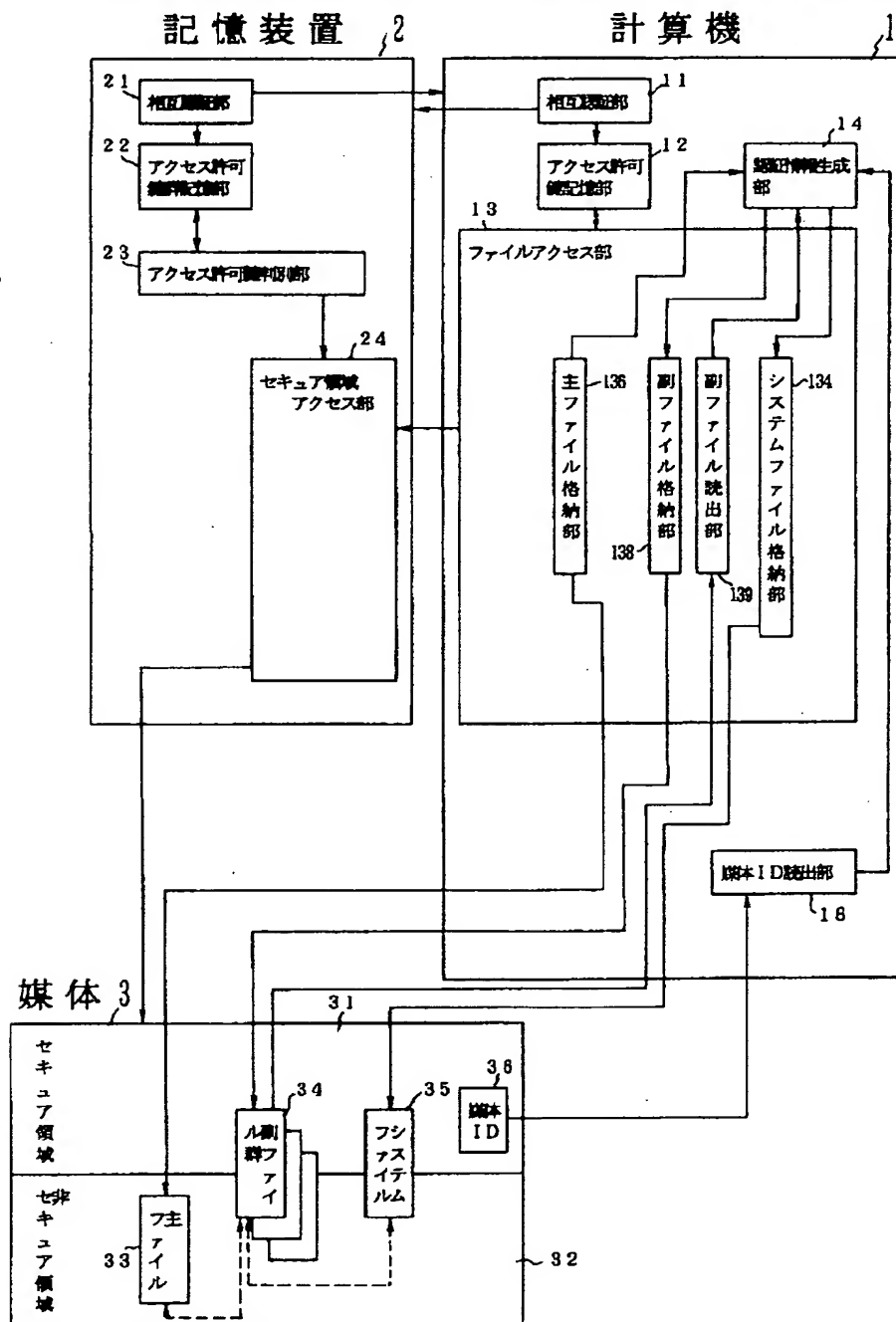
【図13】

本発明の第5の実施の形態における動作フローチャート



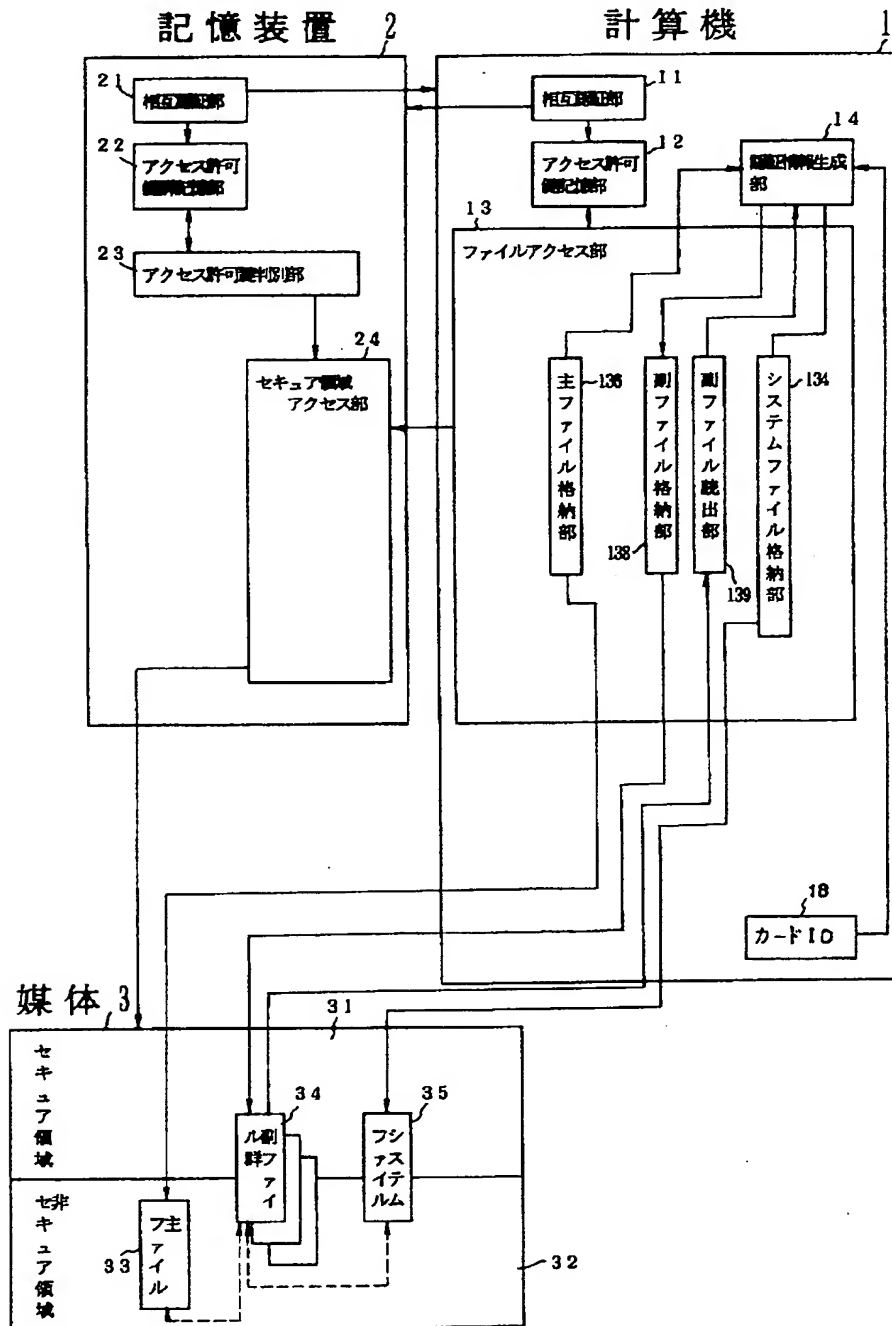
【図12】

本発明の第5の実施の形態における改ざん防止/
検出機能を有するファイル管理システムの構成図



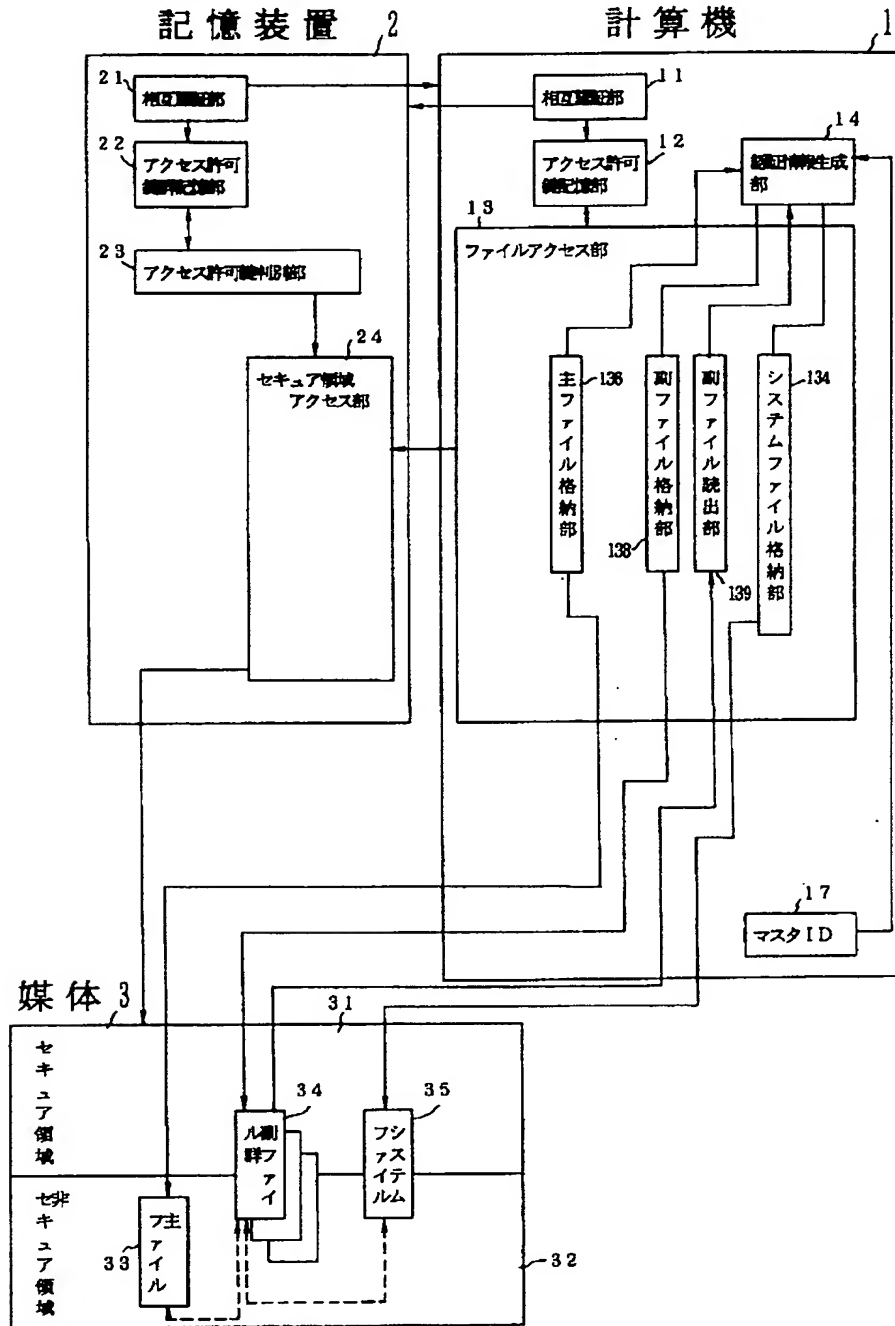
【図14】

本発明の第6の実施の形態における改ざん防止/
検出機能を有するファイル管理システムの構成図



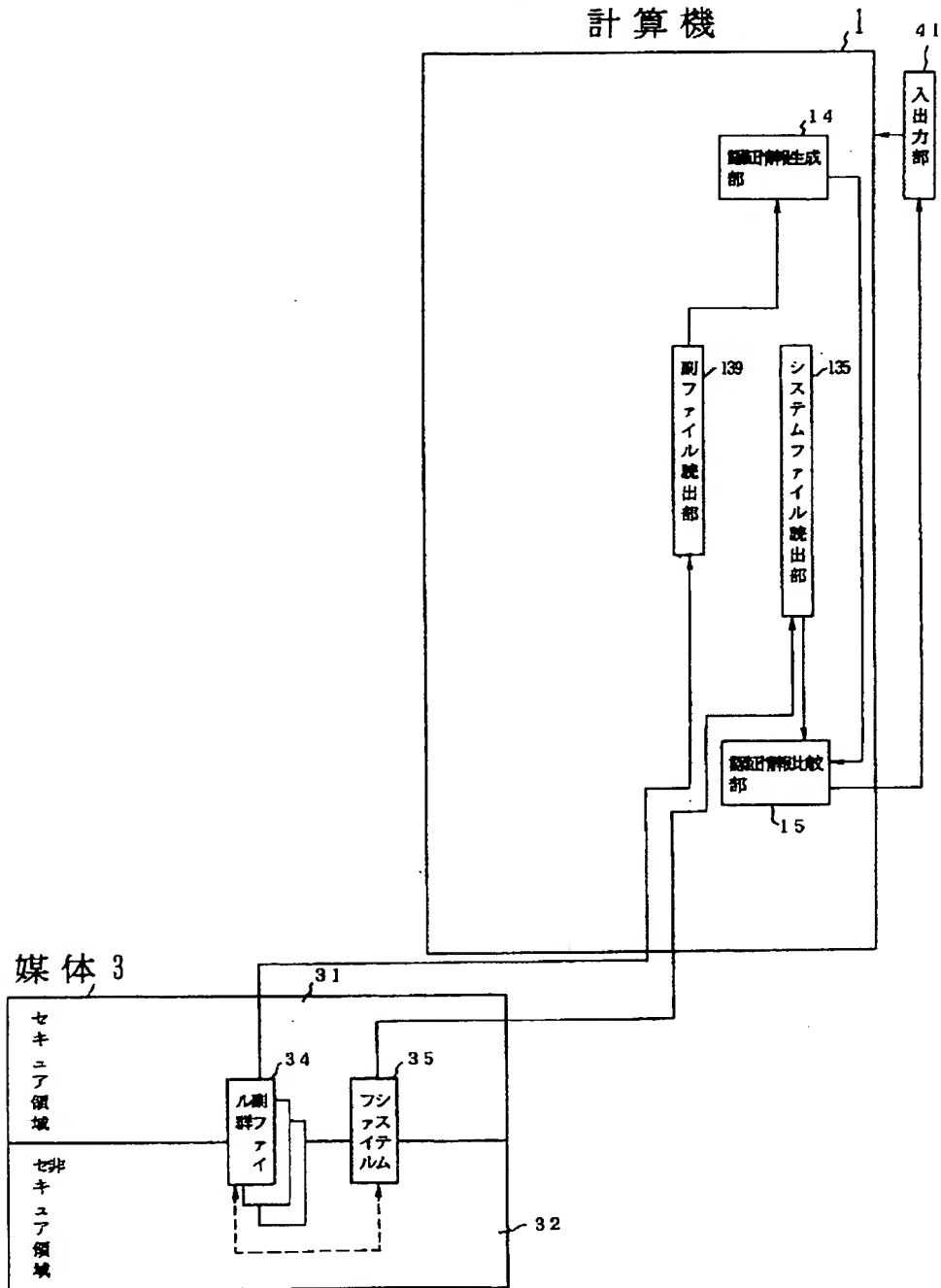
【図15】

本発明の第7の実施の形態における改ざん防止/
検出機能を有するファイル管理システムの構成図



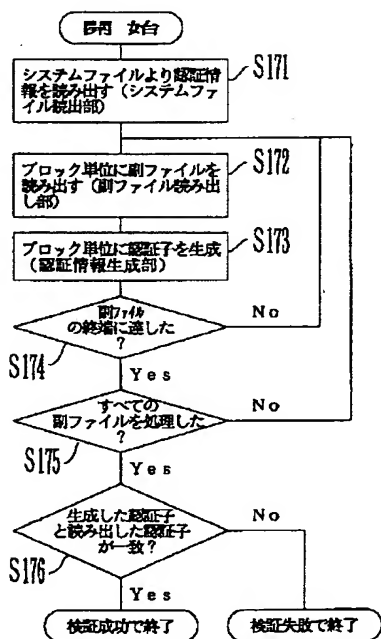
【図16】

本発明の第8の実施の形態における改ざん防止/
検出機能を有するファイル管理システムの構成図



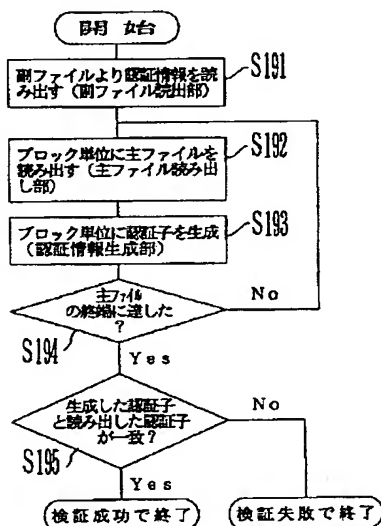
【図17】

本発明の第8の実施の形態における動作フローチャート



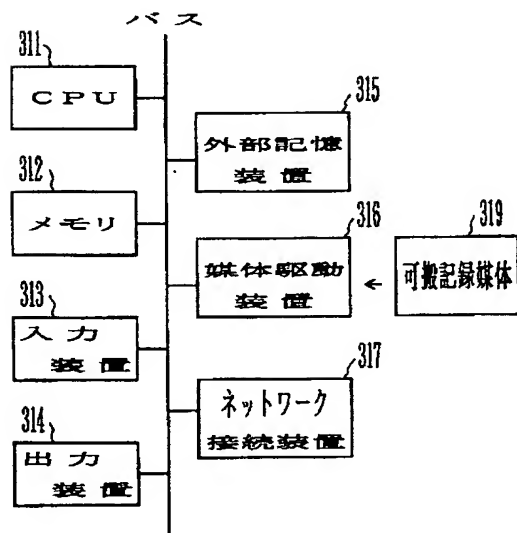
【図19】

本発明の第9の実施の形態における動作フローチャート



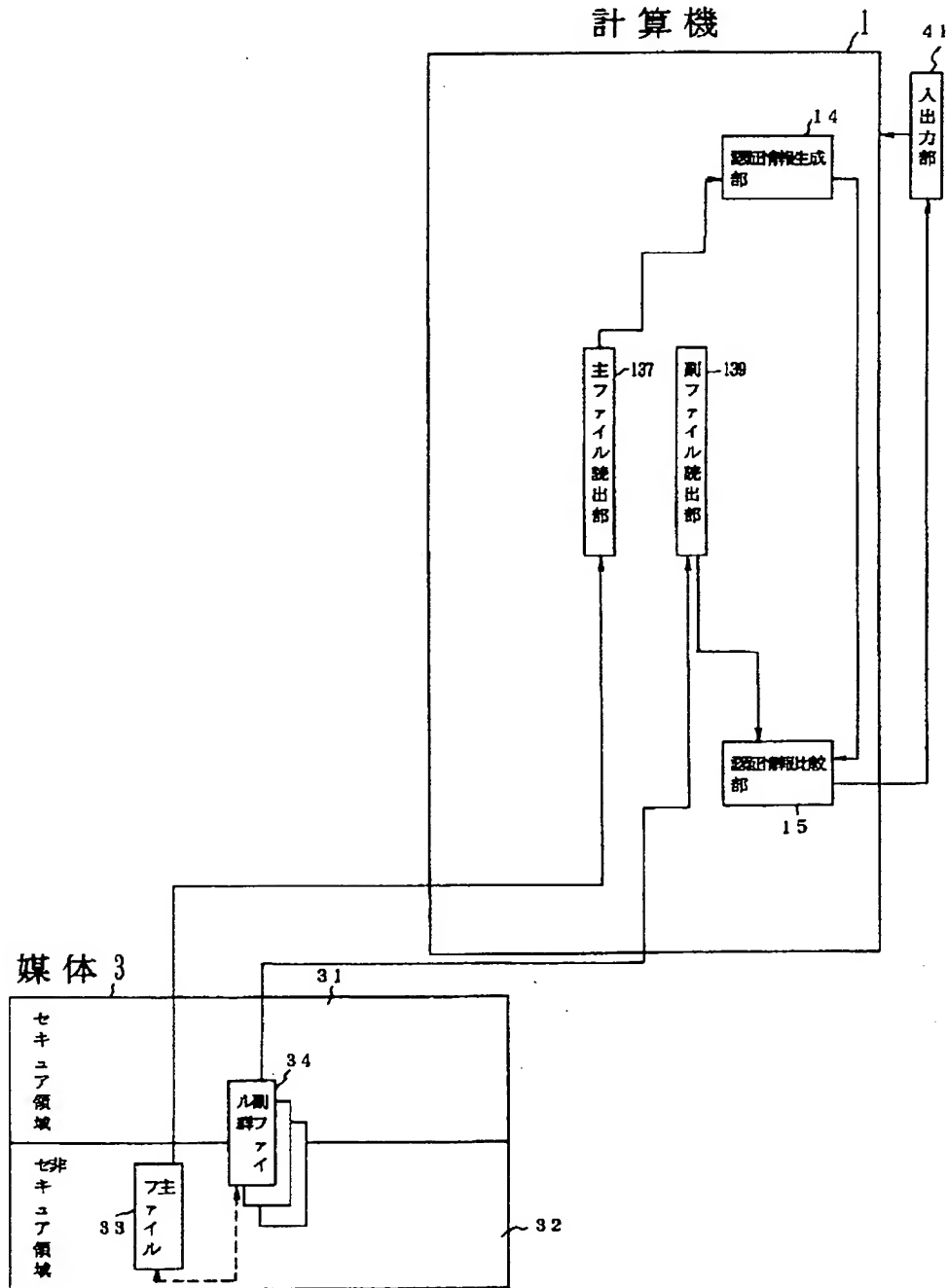
【図31】

改ざん防止/検出システムの構成図



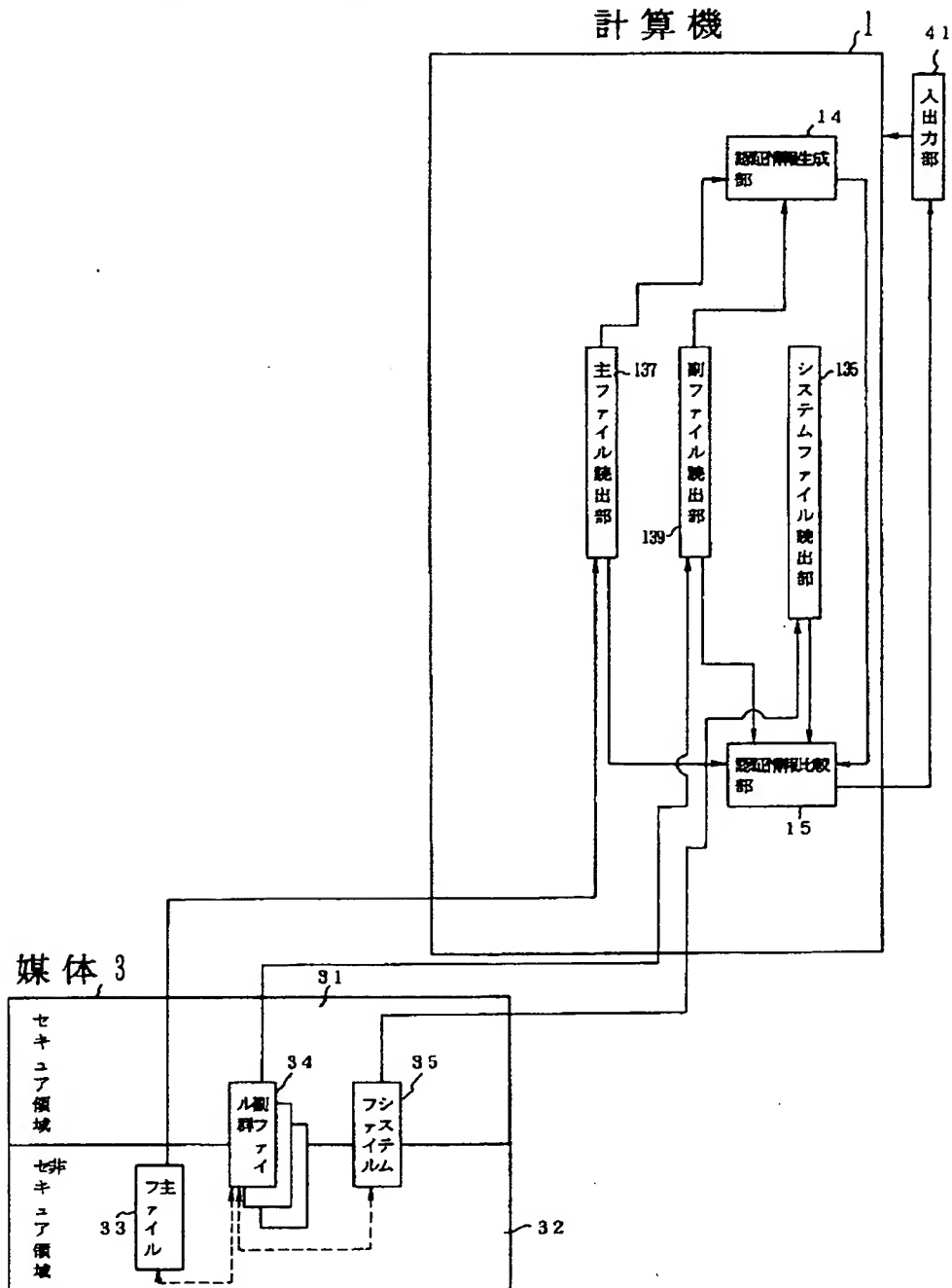
【図18】

本発明の第9の実施形態における改ざん防止/
検出機能を有するファイル管理システムの構成図



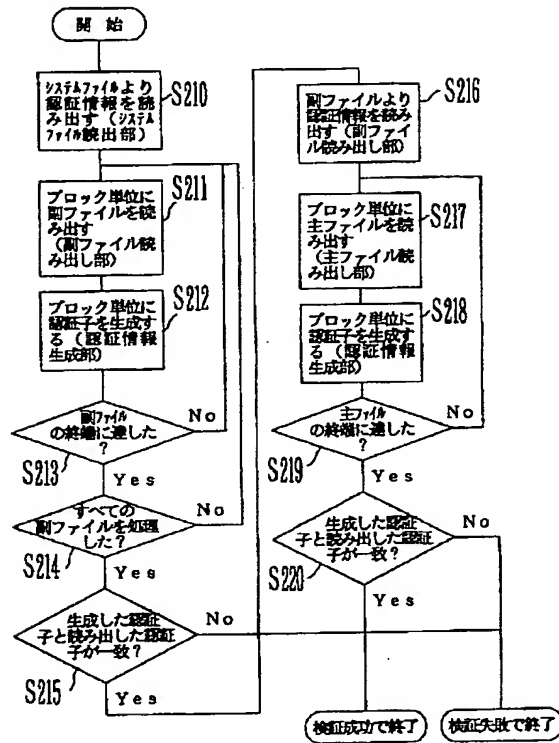
【図20】

本発明の第10の実施の形態における改ざん防止/
検出機能を有するファイル管理システムの構成図



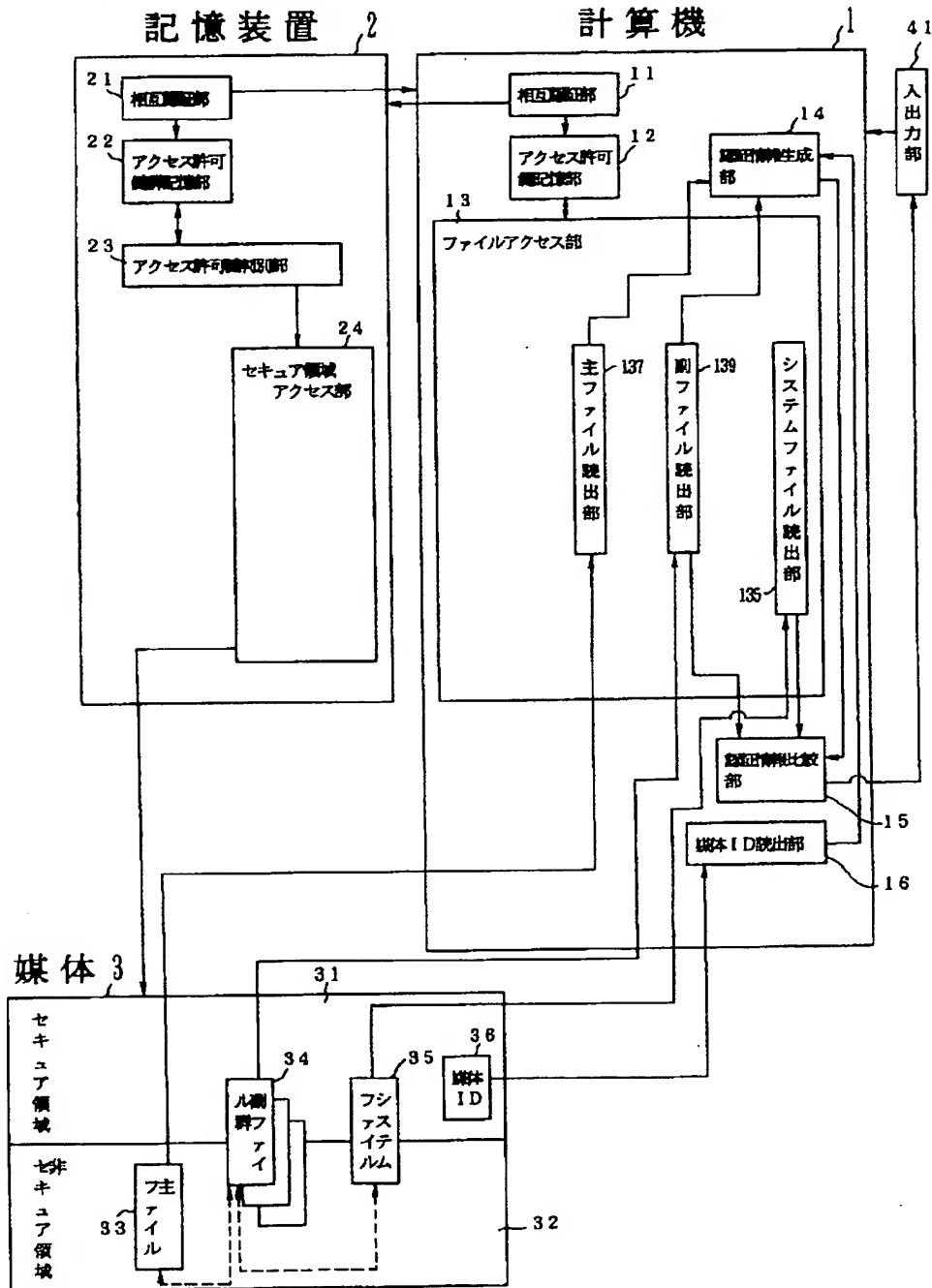
【図21】

本発明の第10の実施形態における動作フローチャート

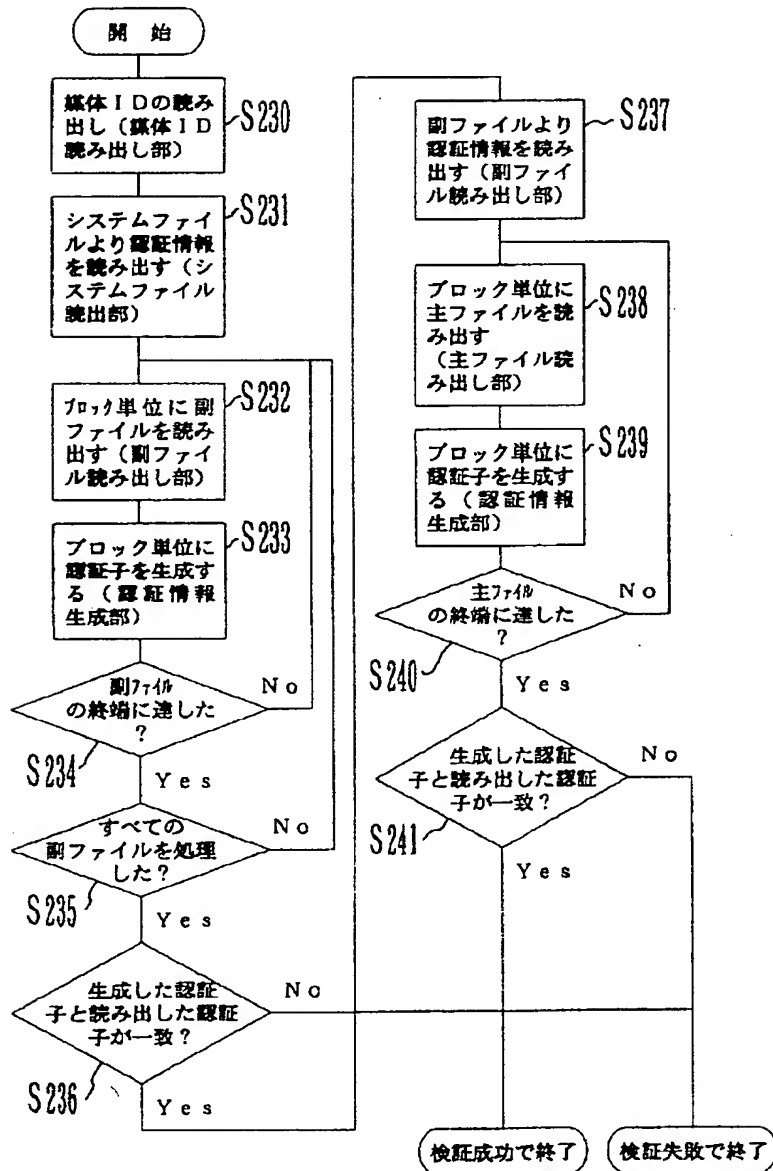


【図22】

本発明の第11の実施の形態における改ざん防止/
検出機能を有するファイル管理システムの構成図

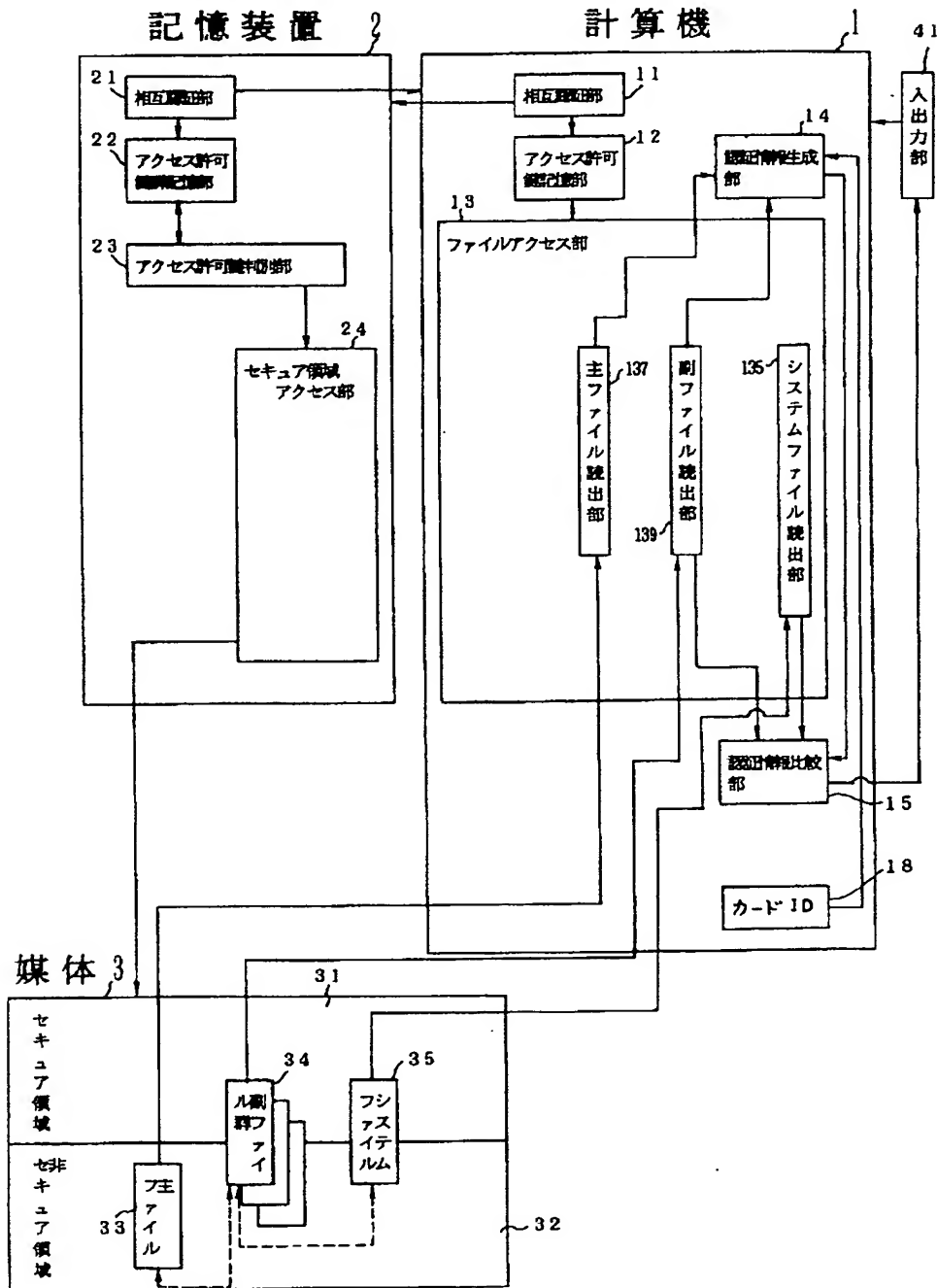


【図23】

本発明の第1の実施形態における
動作フローチャート

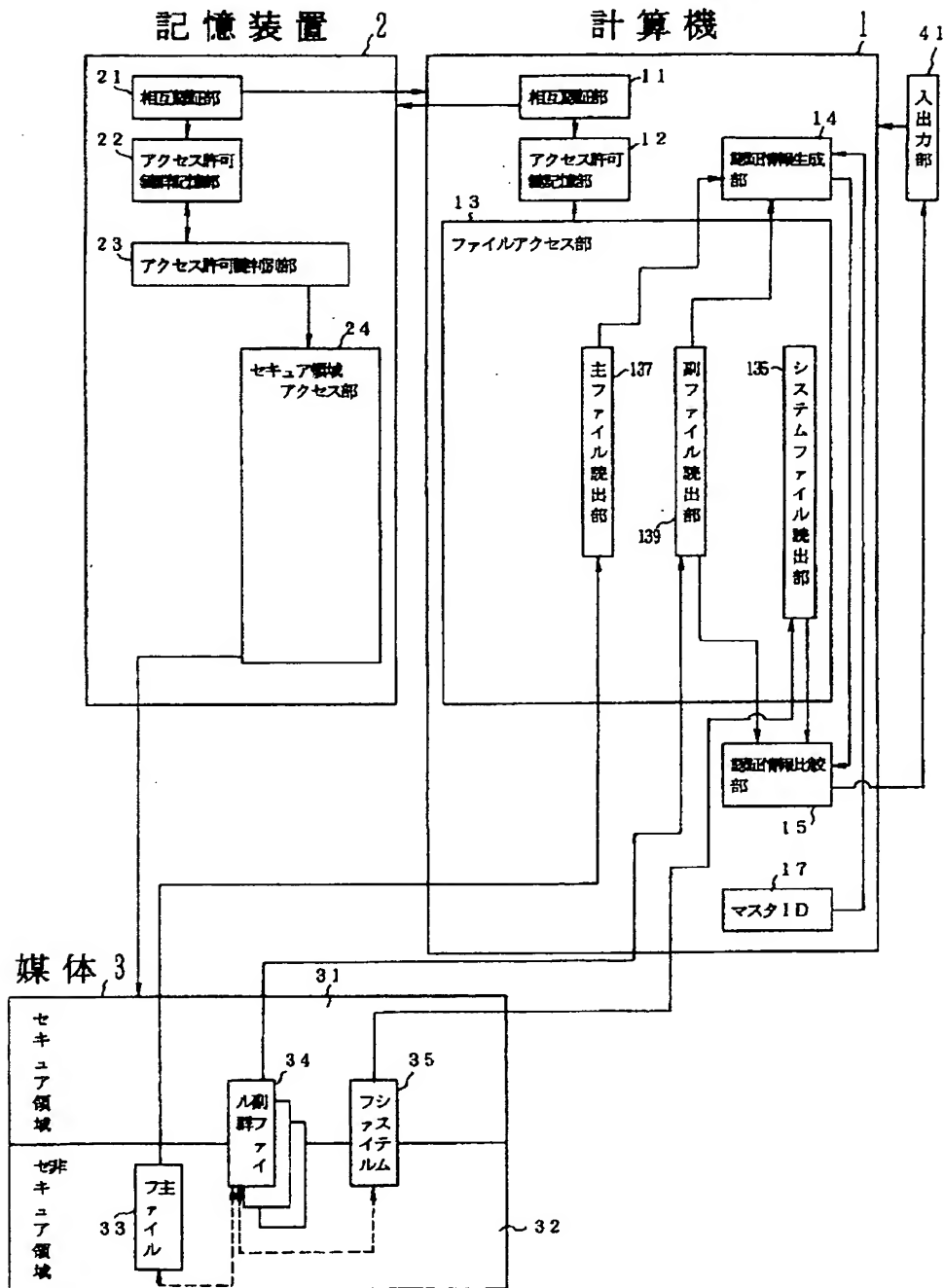
【図24】

本発明の第12の実施の形態における改ざん防止/
検出機能を有するファイル管理システムの構成図



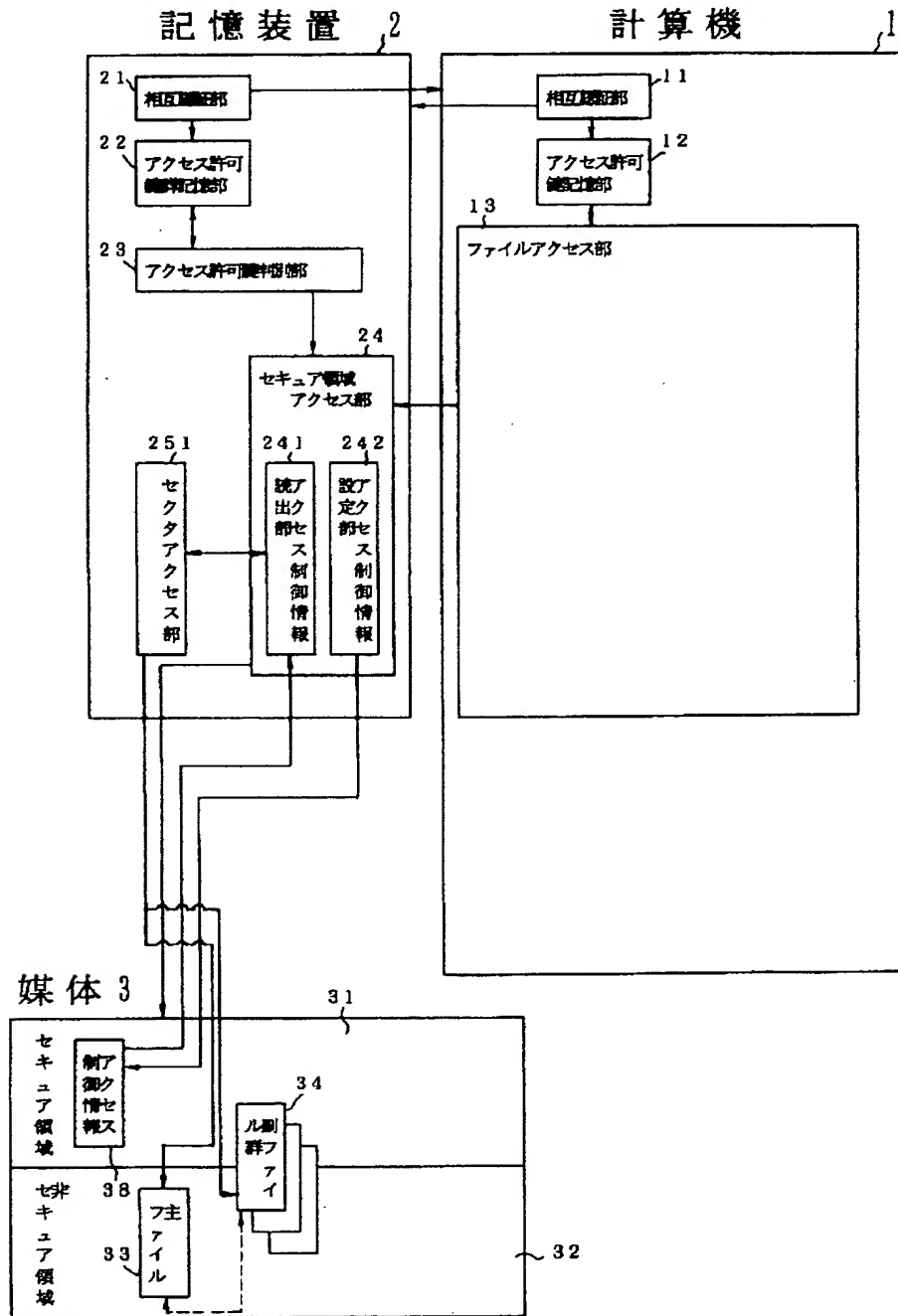
【図25】

本発明の第13の実施の形態における改ざん防止/
検出機能を有するファイル管理システムの構成図



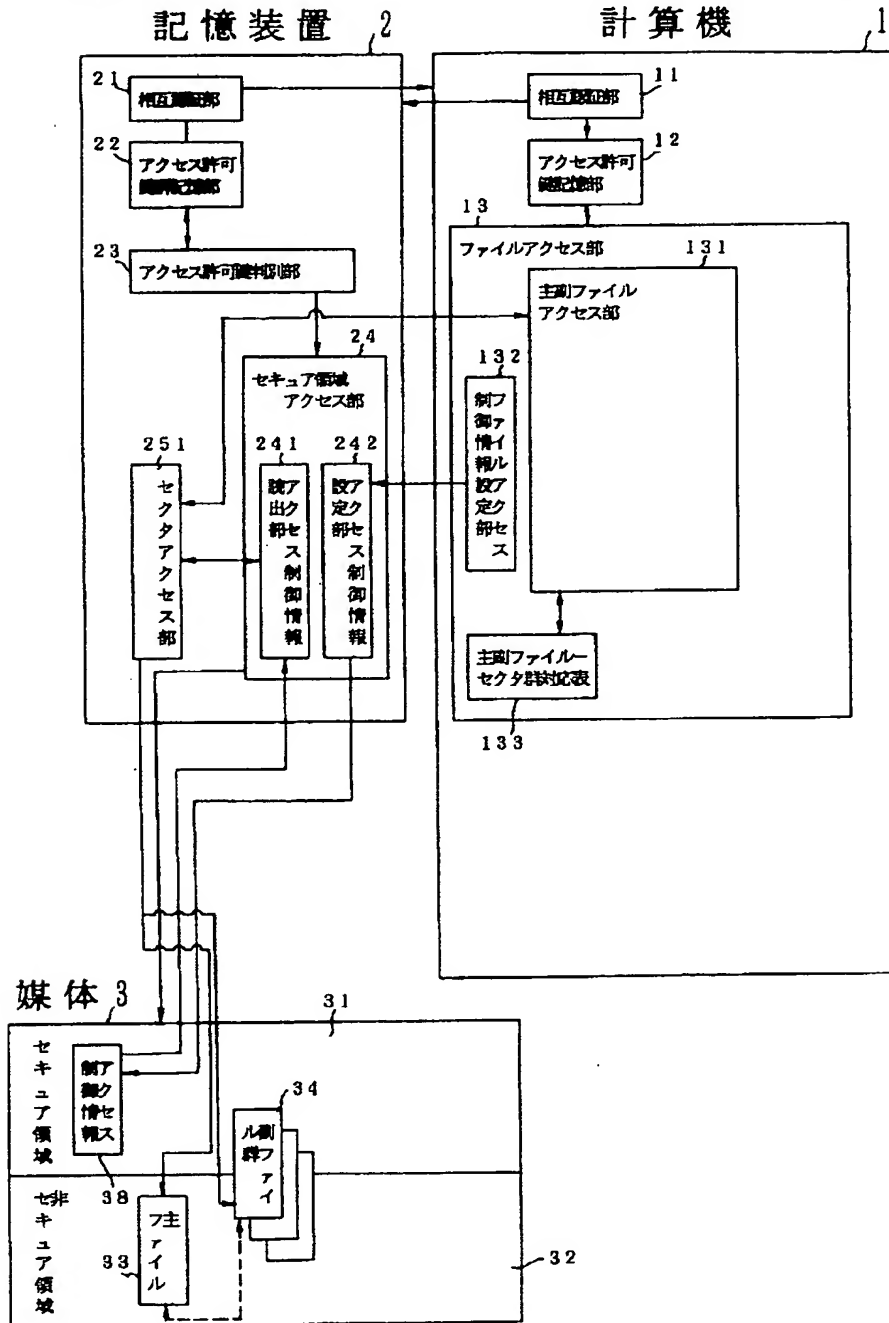
【図26】

本発明の第14の実施の形態における改ざん防止/検出機能を有するファイル管理システムの構成図



【図28】

本発明の第15の実施の形態における改ざん防止/
検出機能を有するファイル管理システムの構成図



【図30】

本発明の第16の実施の形態における改ざん防止/
検出機能を有するファイル管理システムの構成図

